Net-Centric Implementation Framework

Part 1: Overview

Part 2: ASD(NII) Checklist Guidance

Part 3: Migration Guidance

Part 4: Node Guidance

Part 5: Developer Guidance

Part 6: Acquisition Guidance

V 1.3

16 June 2006

Net-Centric Enterprise Solutions for Interoperability (NESI) is a collaborative activity of the USN PEO for C4I and Space, the USAF Electronic Systems Center, and the Defense Information Systems Agency.

Approved for public release; distribution is unlimited.

Table of Contents

1 NESI Implementation

This section contains NESI background information. For a more complete overview, see the first part of the NESI document set, *NESI Part 1: Overview*. Section 2 of *NESI Part 4: Node Guidance* (this document) presents a set of Perspectives which are a means of organizing and presenting information concerning nodes and encapsulating pertinent guidance and best practices associated with each perspective topic. Note that the best practice statements in this version of Part 4 have a BP number (e.g., [BP1234])which will link to best practice details in a subsequent version (as in *NESI Part 5: Developer Guidance*).

1.1 References

(a) DoD Directive 5000.1, *The Defense Acquisition System*, 24 November 2003.

(b) DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, 12 May 2003.

(c) DoD Directive 8100.1, *Global Information Grid (GIG) Overarching Policy*, 21 November 2003.

(d) DoD Directive 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 05 May 2004.

(e) DoD Instruction 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004.

(f) DoD Directive 5101.7, *DoD Executive Agent for Information Technology Standards*, 21 May 2004.

(g) *DoD Global Information Grid (GIG) Architecture, Version 2.0*, August 2003.

(h) *DoD Architecture Framework (DoDAF), Version 1.0*, 9 February 2004.

(i) *DoD Net-Centric Data Strategy*, DoD Chief Information Officer, 9 May 2003.

(j) CJCSI 3170.01E, *Joint Capabilities Integration and Development System*, 11 May 2005.

(k) CJCSM 3170.01B, *Operation of the Joint Capabilities Integration and Development System*, 11 May 2005.

(l) CJCSI 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems*, 8 March 2006.

(m)*Net-Centric Operations and Warfare Reference Model (NCOW RM) V1.0*, September 2003.

(n) *Net-Centric Checklist, V2.1.3*, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 12 May 2004.

(o) *A Modular Open Systems Approach (MOSA) to Acquisition, Version 2.0*, September 2004.

(p) DoD IT Standards Registry (DISR), http://disronline.disa.mil.

(q) *Net-Centric Attributes List*, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, June 2004.

(r) *Global Information Grid (GIG) Key Interface Profiles (KIPs) Framework (DRAFT)*, Version 0.95, 7 October 2005.

1.2 Overview

Net-Centric Enterprise Solutions for Interoperability (NESI) provides, for all phases of the acquisition of net-centric solutions, actionable guidance that meets DoD Network-Centric Warfare goals. The guidance in NESI is derived from the higher level, more abstract concepts provided in various directives, policies and mandates such as the *Net-Centric Operations and Warfare Reference Model* (*NCOW RM*) and the ASD(NII) *Net-Centric Checklist*, references (m) and (n), respectively. As currently structured, NESI guidance is captured in documents covering architecture, design and implementation; a compliance checklist; and a collaboration environment that includes a repository of guidance statements and code examples.

More specifically, NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for military application. NESI provides specific technical recommendations that a DoD organization can use as references. Stated another way, NESI serves as a reference set of compliant instantiations of these directives.

NESI is derived from a studied examination of enterprise-level needs and, more importantly, from the collective practical experience of recent and on-going program-level implementations. It is based on today's technologies and probable near-term technology developments. It describes the practical experience of system developers within the context of a minimal top-down technical framework. Most, if not all, of the guidance in NESI is in line with commercial best practices in the area of enterprise computing.

NESI applies to all phases of the acquisition process as defined in references (a) and (b) and applies to both new and legacy programs. NESI provides explicit counsel for building in net-centricity from the ground up and for migrating legacy systems to greater degrees of net-centricity.

NESI subsumes a number of references and directives; in particular, the Air Force *C2 Enterprise Technical Reference Architecture (C2ERA)*[1] and the Navy *Reusable Applications Integration and Development Standards (RAPIDS)*.[2] Initial authority for NESI is per the Memorandum of Agreement between Commander, Space and Naval Warfare Systems Command (SPAWAR), Navy PEO C4I & Space and the United States Air Force Electronic Systems Center, dated 22 December 2003, Subject: Cooperation Agreement for Net-Centric Solutions for Interoperability (NESI). The Defense Information Systems Agency (DISA) formally joined the NESI effort in 2006.

1.3 Releasability Statement

This document has been cleared for public release by competent authority in accordance with DoD Directive 5230.9 and is granted *Distribution Statement A: Approved for public release; distribution is unlimited*. Obtain electronic copies of this document at http://nesipublic.spawar.navy.mil.

[1] Air Force C2 Enterprise Technical Reference Architecture, v3.0-14, 1 December 2003.

[2] RAPIDS Reusable Application Integration and Development Standards, Navy PEO C4I & Space, December 2003 (DRAFT V1.5).

1.4 Vendor Neutrality

The NESI documentation sometimes refers to specific vendors and their products in the context of examples and lists. However, NESI is vendor-neutral. Mentioning a vendor or product is not intended as an endorsement, nor is a lack of mention intended as a lack of endorsement.

Code examples typically use open-source products since NESI is built on the open-source philosophy. NESI accepts inputs from multiple sources so the examples tend to reflect whatever tools the contributor was using or knew best. However, the products described are not necessarily the best choice for every circumstance. Users are encouraged to analyze specific project requirements and choose tools accordingly. There is no need to obtain, or ask contractors to obtain, the open-source tools that appear as examples in this guide. Similarly, any lists of products or vendors are intended only as references or starting points, and not as a list of recommended or mandated options.

1.5 Disclaimer

Every effort has been made to make NESI documentation as complete and accurate as possible. Even with frequent updates, this documentation may not always immediately reflect the latest technology or guidance.

1.6 Contributions and Comments

NESI is an open-source project that will involve the entire development community. Anyone is welcome to contribute comments, corrections, or relevant knowledge to the guides via the Change Request tab on the NESI Public site, http://nesipublic.spawar.navy.mil, or via the following email address: nesi@spawar.navy.mil.

1.7 Collaboration Site

The Navy has established a collaboration site to support NESI community interaction. It is located at https://nesi.spawar.navy.mil (user registration required). Use this site for collaborative software development across distributed teams.

2 Nodes

A Node is a collection of Components (i.e., systems, applications, services and other Nodes) which results from the alignment of organizations, technologies, process, or functions. Potential alignment attributes include management, acquisition, mission, technological, sustainment, spatial, or temporal. A Node enables the sharing of common approaches that support net-centric interoperability. As a concept, Nodes may not be defined in terms of a concrete set of Components or size.

The presumption is that Nodes are actively managed. The shared capabilities necessary to support net-centric interoperability could be provided either by the Node or a system within the Node (i.e., the system is acting as executive agent for the capability).

The discussion of NESI Node guidance is presented in the following perspectives and is largely consistent with the Key Interface Profile (KIP) Framework (DRAFT):

- General Responsibilities
- Node Transport
- Node Computing Infrastructure
- Node Application Enterprise Services

Factors such as physical environments and employment concepts directly influence the scope of a Node, and boundaries and can vary widely. As a notional example, consider whether an individual foot soldier should be considered a Node. While soldiers are increasingly being outfitted with sensors and computing devices, it is unlikely (in the near term) than an individual soldier could host the requisite capabilities needed to ensure compliance with, for instance, the DoD IA Strategy including intrusion detection, firewalls, and such. Rather, a collection of soldiers such as an infantry battalion would be connected to a field command center that provides the requisite infrastructure. Note that this does not preclude an individual soldier form being directly addressable on the Global Information Grid (GIG), able to conduct information exchanges on a global scale. It simply means that requisite infrastructure is unlikely to be isolated to the soldier but rather shared with others. Likewise, nothing precludes the soldier from being a full Node should technology enable the soldier to carry all the requisite infrastructure elements.

> ***Note***: A Node might be nested; such cases would likely introduce additional complexities that would require extra management attention and coordination.

The guidance and best practices in these perspectives is meant for those in a position to influence decisions regarding infrastructure and services provided by the Node for shared use by the systems within the Node. With respect to the GIG, the principal question addressed is how should a Node implement the shared infrastructure needed to achieve the DoD vision of broad integration and interoperability across the GIG, on behalf of systems within the Node, and in accordance with DoD policy and direction?

The guidance is applicable to *information systems*, such as those for command and control or intelligence. It may also be applicable, in part or whole, to other classes of systems or variants, such as embedded or real-time systems, but is aimed principally at systems that have desktop computers, servers, email, Web browsers and such.

Multiple operating environments are considered in the guidance including but not limited to fixed, deployed, mobile air/land/sea Nodes or other instance specific implementations. Occasionally, guidance may be provided for a specific environment or instance of a Node.

2.1 General Responsibilities

In addition to the specific requirements of a NESI Node to support transport, common computing infrastructure, Enterprise Services and Community of Interest (COI) services there are some general responsibilities that a NESI Node must support in order to ensure that the final product can interact with the rest of the Global Information Grid (GIG). The responsibilities include the following:

- Nodes as Stakeholders
- Net-Centric Information Engineering
- Internal Component Environment
- Integration of Legacy Systems
- Orchestration with External Enterprise
- Orchestration of Internal Components

2.1.1 Nodes as Stakeholders

A Node should be formally represented as a stakeholder in the acquisition and evolutionary activities of all the Components it will host. A Node's Component composition will change in the future; maintain and identify all the known Components throughout the lifecycle of the Node. This action is fundamental to the provisioning of a shared infrastructure and the avoidance of functional duplication within the Node.

The necessity of a Node involvement as a stakeholder in its Components may not be obvious; it has a bearing on Global Information Grid (GIG) interoperability. Component independent planning and evolution is likely to result in the external exposure of inconsistencies or, worse, incomplete, inaccurate, or misunderstood data. Consider two systems within the Node that both ingest a particular type of data, but process it at different levels of fidelity, and are independently intending to publish the result to the rest of the GIG. This is an example of when a Node manager would want to work across the systems to ensure that the Node presents its collective capability clearly.

Best Practices

- A Node should have a comprehensive list of all the Components that will part of its composition. [BP1569]

- Node management should assume a role among the Components within the Node. [BP1570]

2.1.2 Net-Centric Information Engineering

Of particular concern for Global Information Grid (GIG) interoperability is the information contained in inter-nodal information exchanges. Information exchanges are typically the purview of the systems within the Node, rather than the Node itself, and the details are worked out by a Community of Interest (COI). But the Node infrastructure must be engineered to support information exchanges between various COIs. The COIs can require any number of Components to fulfill the mission, When a Component wishes to make its data available to the enterprise, there are different enterprise design patterns which can be used. For example, the mechanism selected by a Component to exchange information may be publish-subscribe, broker, or client server. The Node infrastructure must support whichever enterprise design pattern mechanism is selected. Consequently, the Node has a stake in the Component design. Additionally, the Node has a stake in performance specifications provided in the Service Level Agreements (SLA). The SLA is a contract that commits the application service provider to a required level of service. The Node must support that level of service with its infrastructure.

Node management should designate COI representatives to track, advocate, and engineer information exchanges in support of the DoD Net-Centric Data Strategy. According to this strategy, "COI is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange." The principal mechanism for recording COI agreements is the DoD Metadata Registry required by the DoD CIO "DoD Net-Centric Data Management Strategy: Metadata Registration" memo. There are registry implementations on the Non-secure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS).

The DoD Metadata Registry Web site provides a search capability. There is also a SOAP based interface to the Registry.

Best Practices

- A Node should have a comprehensive list of all the Communities of Interests (COIs) to which the Node's Components belong. [BP1571]

- A Node should be party to any Service Level Agreements (SLAs) signed by any of its components. [BP1572]

- A Node should define which enterprise design patterns it supports. [BP1573]

- A Component should define which enterprise design patterns it requires. [BP1574]

- Node management should designate representatives to relevant Communities of Interests (COIs). [BP1575]

2.1.3 Internal Component Environment

Nodes should provide an environment to support the development, integration, and testing of net-centric capabilities of its Components. As Nodes themselves and the Components within the Nodes move closer to the implementation of net-centric capabilities, it becomes increasingly important to provide a development, integration, and test environment to support those capabilities. This environment should allow for the exercise not just the Node infrastructure, but also either host locally within the Node, or provide access to, Net-Centric Enterprise Services (NCES) piloted services. The particulars on how this is done depend on the characteristics of the

Node. For example, mobile or deployed Nodes would provide environments substantially different than fixed land-based or permanent Nodes.

At the earliest opportunity within the Node and Component lifecycles developers should be using the NCES piloted Enterprise Services offered by DISA for development, test, and integration. In the absence of a Node-provided environment, Component developers should use the piloted services directory, through an early adopter agreement, but use of a Node-provided environment at the earliest opportunity is preferable to minimize problems. Potential causes of problems include security parameters, network configuration, and product inconsistencies.

DISA has published an NCES Pilot Participant’s Guide that describes the process for using the piloted services.

Best Practices

- Nodes should provide an environment to support the development, build, integration, and test of net-centric capabilities. [BP1576]
- Nodes should define an enterprise service schedule for interim and final enterprise capabilities. [BP1577]
- Components should define a schedule that covers the use of the Enterprise Services defined within the Node’s Enterprise Service schedule. [BP1578]
- Nodes should define which Enterprise Services will be hosted by the Node locally when the Node becomes operational. [BP1579]
- Nodes should define which Enterprise Services will be hosted over the Global Information Grid (GIG) when the Node becomes operational. [BP1580]

2.1.4 Integration of Legacy Systems

Nodes might contain systems or applications that are in the Sustainment lifecycle phase. These Components are often referred to as “legacy” systems or applications. Changing the internals of such Components to support net-centricity is impractical and offer has little return on investment. Usually, the decisions to brand a system or an application as a “Legacy” system is made at a high level in conjunction with the operational user and acquisition communities. When the legacy functionality needs to be exposed as an interim solution internally to a Node or external to the Node as a proxy it is often accomplished using service that uses a façade technique. The façade technique is often implemented using a wrapper or an adapter design pattern around the existing legacy system or application.

Best Practice

- Expose legacy system or application functionality through the use of service that uses a façade design pattern. [BP1581]

2.1.5 Orchestration of Node and Enterprise Services

The Net-Centric Enterprise Services (NCES) capabilities under definition, development, or in pilot testing are complex and use leading edge technologies. The status, availability and deployment schedule for services should be reflected in an integrated master schedule for the

Node that shows planned dependencies of systems within the Node on these services. Given the rate of evolution and leading edge nature of some services, the orchestration of efforts should be detailed, including specific version numbers, workarounds, assumptions, constraints, configuration, and best practices. Note that these practices should be followed for orchestration with both external and Node provided Enterprise Services.

Best Practices

- Nodes should define an enterprise service schedule for interim and final enterprise capabilities. [BP1577]

- Components should define a schedule that covers the use of the Enterprise Services defined within the Node's Enterprise Service schedule. [BP1578]

- Enterprise Services schedules should include version numbers of standard Enterprise Services interfaces being implemented [BP1582]

2.1.6 Orchestration of Internal Components

The shared infrastructure provided by Nodes, for shared use by its member Components cannot evolve independently of the Components within the Node. Nodes may host a variety of Components and Components may be members of multiple Nodes. Consequently, Components are likely to be developed with differing timeframes and rates of evolution. This presents a coordination challenge for the Node managers.

Best Practice

- A Node should routinely provide Enterprise Services schedule updates to its entire member Components. [BP1583]

2.2 Node Transport

A Node provides a transport infrastructure that is shared among the Components within the Node, implements Global Information Grid (GIG) IA boundary protections, and is Internet Protocol Version 6 (IPv6) capable. In some cases, guidance may seem rudimentary, but history demonstrates that configuration errors for such rudimentary aspects are often the cause of interoperability, integration, and information assurance issues.

The DISA/National Security Agency (NSA) Security Technical Implementation Guidance (STIG) documents are applicable in several places throughout this section. The guidance provided by those documents is not repeated here. The STIG documents are updated frequently as new vulnerabilities are discovered and the current "state of the art" is refined. The applicable STIG documents should be consulted as a fundamental part of design activities, and monitored periodically for updates.

Transport elements provided by a Node are obviously essential in achieving net-centricity but also play a key role in minimizing interoperability issues. The Transport elements are described in the following perspectives:

- Internet Protocol (IP)
- Domain Name System (DNS)
- Routers

- Time Services
- Mobile and Dynamic Networks
- Multicast
- Network Information Assurance Components
- Enterprise Management Services
- Virtual Private Networks (VPN)
- Trusted Guards
- Integration of Non-TCP/IP Transports
- Black Core

Note: The elements described above are in a recommended order of implementation, with the basic enablers described first, for a notional Node. Specific elements and implementation order may vary according to factors such as Node connectivity, scale, mission, and concepts of employment.

Best Practices

- Nodes should provide a transport infrastructure that is shared among Components within the Node. [BP1584]

- Nodes should provide a transport infrastructure that is implements Global Information Grid (GIG) Information Assurance (IA) boundary protections. [BP1585]

- The applicable Security Technical Implementation Guidance (STIG) documents should be consulted as a fundamental part of design activities, and monitored periodically for updates. [BP1701]

References

- DoD CIO memos:
  - 9 June 2003, “Internet Protocol Version 6 (IPv6)”
  - 29 September 2003, “Internet Protocol Version 6 (Ipv6) Interim Transition Guidance”
  - 28 November 2003, “Internet Protocol Version 6 (IPv6) Transition Plan Coordination and Interim Tasking”
  - Aug. 16 2005 “Internet Protocol Version 6 (Ipv6) Policy Update”
  - 16 August 2005, “DoD Internet Protocol Version 6 (IPv6) Pilot Nominations”

2.2.1 Internet Protocol (IP)

The Assistant Secretary of Defense for Networks and Information Integration, ASD(NII), defines Internet Protocol (IP) as one of nine attributes of net-centricity. It is among the most fundamental of protocols needed for Global Information Grid (GIG) interoperability. There are, however, a number of interoperability challenges emerging as DoD usage of IP networking continues to expand. Two of these areas are the following:

- IPv4 to IPv6 Transition

- Mobile Nodes

2.2.1.1 IPv4 to IPv6 Transition

A 9 June 2003 ASD(NII)/DoD CIO memo, "Internet Protocol Version 6 (IPv6)," is the first in a series of memos (see the References below) addressing DoD transition to IPv6 and establishing IPv6, as the next generation network protocol for DoD with the transition date goal of FY 2008. The DoD IPv6 Transition Office created in DISA is responsible for master transition plan development, acquiring Internet Protocol (IP) addresses, providing necessary infrastructure and technical guidance, and ensuring that unified solutions are used across DoD to minimize the cost and interoperability issues. DoD components are tasked with the development of the component transition plans and with providing guidance and governance to programs. Three main Milestone Objectives (MOs)[3] have been outlined for the gradual and controlled transition of the enterprise. Currently only those systems approved as MO1 pilots are allowed to switch to IPv6 in operational environments.

To enable this transition, as of 1 October 2003 all Global Information Grid (GIG) assets being developed, procured, or acquired shall be IPv6 capable (while retaining compatibility with IPv4). The DoD IPv6 Working Group is working on IPv6 implementation issues through formal standards bodies by. A high level working definition for "IPv6 capable" is available; the list of the standard IPv6 specifications approved for the use in DoD networks is hosted on DISR[4] website.

An IPv6 transition plan should be prepared for the Node infrastructure as well as the transport users within the Node in coordination with the Component and DoD transition plan; the plan might have to be reviewed and approved by the appropriate IPv6 transition authority. Coordination is essential to ensure that the intermediate network infrastructures are IPv6 capable in the planned timeframe, and similarly for other-end network infrastructures for known system interfaces. The Node's IPv6 transition plan should consider applicable DoD Component IPv6 transition plans, IPv6 working group products, and include interoperability testing in the plan. The net-centric concepts of loose coupling and discoverable services may be impacted by the transition to IPv6 if services begin depending on IPv6-specific features. Services that have been developed to utilize IPv6 features and which may perform differently if accessed via an Internet Protocol Version 4 (IPv4) infrastructure should describe the potential impacts in the Service Registry.

IPv6 transition has an impact on many transport infrastructure components. The IPv6 Transition Plan for a Node should include transition of all impacted network elements including DNS, routing, security, and dynamic address assignment. The DoD IPv6 Network Engineer's Guidebook (Draft) and the DoD IPv6 Application Engineer's Guidebook (Draft) provide guidance for transition of impacted components.

Best Practices

- Nodes should provide a transport infrastructure that is Internet Protocol Version 6 (IPv6) capable in accordance with the appropriate governing transition plan. [BP1586]

[3] March 2005, "The Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan"

[4] DoD IT Standards Registry (DISR), http://disronline.disa.mil

- An Internet Protocol Version 6 (IPv6) transition plan should be prepared for the Node. [BP1587]

- An Internet Protocol Version 6 (IPv6) transition plan should coordinate with the Components that comprise the Node. [BP1588]

- The Internet Protocol Version 6 (IPv6) transition plan for a Node should address issues in the applicable governing DoD component IPv6 transition plans. [BP1589]

- The Node's Internet Protocol Version 6 (IPv6) transition plan should prepare IPv6 Working Group products. [BP1591]

- The Node's Internet Protocol Version 6 (IPv6) transition plan should include interoperability testing in the plan. [BP1592]

- The Node's Internet Protocol Version 6 (IPv6) Transition Plan should include transition of all the impacted elements of the network. [BP1590]

    - A Node Domain Name System (DNS) must support both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) simultaneously. [BP1599]

    - Design DNS infrastructure in accordance with appropriate governing IPv6 Transition Office requirements. [BP1705]

    - Any Internet Protocol Version 6 (IPv6) address used on DoD systems must be originated at DISA. [BP1600]

- Services that have been developed to utilize Internet Protocol Version 6 (IPv6) features and which may perform differently if accessed via an Internet Protocol Version 4 (IPv4) infrastructure should describe the potential impacts in the Service Registry. [BPND0025]

References

- DoD CIO memos:
    - 9 June 2003, "Internet Protocol Version 6 (IPv6)"
    - 29 September 2003, "Internet Protocol Version 6 (Ipv6) Interim Transition Guidance"
    - 28 November 2003, "Internet Protocol Version 6 (IPv6) Transition Plan Coordination and Interim Tasking"
    - Aug. 16 2005 "Internet Protocol Version 6 (Ipv6) Policy Update"
    - 16 August 2005, "DoD Internet Protocol Version 6 (IPv6) Pilot Nominations"

- March 2005, "The Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan"

- DoD IT Standards Registry (DISR), http://disronline.disa.mil

2.2.1.2 Mobile Nodes

Advances have been made in Transmission Control Protocol/Internet Protocol (TCP/IP) connectivity to mobile Nodes, such as airplanes, ships, and battlefield units, but some significant challenges remain. In particular, it remains unclear to what extent mobile Nodes can directly utilize Enterprise Services, particularly the DISA Core Enterprise Services (CES). The characteristics of the link are likely to be extremely variable, including intermittent connectivity, higher than typical packet loss, low bandwidth, or high latency. Such characteristics are generally problematic for anything but the simplest of Enterprise Services. Components that use these Enterprise Services need to adapt in real-time to the presence or absence of the enterprise service and to the potentially spotty performance of enterprise services. Consequently, the Component must be able to handle the failover and recover from Enterprise Service errors and gaps.

Managers of mobile Nodes that are rely on Internet Protocol (IP) for inter-Node communication should engage with the Net-Centric Enterprise Services (NCES) program office to explore approaches for mobile use of the CES services. Alternatives might include development of specialized Software Development Kits (SDKs) that implement the required adaptive behavior or use of service proxies within the Node that could failover gracefully. Until this topic is explored, the best practice is unknown.

If high bandwidth, high latency satellite communications are employed, the Node should implement the Internet Engineering Task Force Request for Comments 1323, “TCP Extensions for High Performance” (IETF RFC 1323) which addresses describes adjustment of the TCP sliding window buffer to accommodate large amounts of transmitted data that may be in the pipe and not yet unacknowledged due to the long round-trip times of such links. Failure to make this adjustment could result in poor performance and inability to engage in net-centric interoperability.

Best Practice

- Implement IETF RFC 1323 for high bandwidth, high latency satellite communications. [BP1594]

2.2.2 Domain Name System (DNS)

The Domain Name System (DNS) is a system that stores the relationships of host Internet Protocol (IP) address and their corresponding domain names in the equivalent of a distributed database (used here as a simplistic concept). The most import role of the DNS is to map IP addresses to human friendly domain names and back again. For example, **`nesi.spawar.navy.mil`** maps to an Internet Protocol Version 4 (IPv4) address of **`128.49.49.225`** or Internet Protocol Version 6 (IPv6) address: **`1080::34:0:417A`**. For more information on DNS see RFC 1034. DNS also performs other essential functions, such as reverse lookups (obtaining host names from Internet Protocol (IP) addresses, which can be important for security) and email configuration (special DNS Mail eXchange (MX) Records indicate the server used to receive email for a host). These capabilities are fundamental to net-centric operations and are essential for other computing, network, and Enterprise Services.

The DNS namespace is hierarchical. At each level in the hierarchy, the namespace can be further divided into sub-namespaces called zones, which are delegated to other authoritative servers, and which can be further divided and delegated to other authoritative servers, and so on.

Each Node should implement DNS to manage hostname/address resolution within the Node, rather than use hard coded IP addresses, and use the DNS Mail eXchange (MX) Record capabilities to configure electronic mail delivery to the Node.

The DNS implementation should reflect the guidance provided in "Domain Name System Security Technical Implementation Guide". The STIG addresses implementation options such as the choice of basic DNS server types (primary, secondary, caching-only), use of a split-DNS design, location of servers in the network and relationship to other network entities, secure administration, security of zone transfers, and initial configuration.

Operational performance constraints, such as narrow bandwidth and intermittent connectivity should be considered in the design of the Node's DNS. It may be desirable, for instance, to implement a caching-only DNS server for constrained environments.

Best Practices

- Each Node should implement Domain Name System (DNS) to manage hostname/address resolution within the Node. [BP1595]

- Each Node should use the Domain Name System (DNS) Mail eXchange (MX) Record capabilities to configure electronic mail delivery to the Node. [BP1596]

- Operational performance constraints should be considered in the design of the Node's DNS. [BP1597]

- The internal Domain Name System (DNS) service should allow dynamic DNS updates by local Dynamic Host Configuration Protocol (DHCP) server(s). [BP1598]

- A Node Domain Name System (DNS) must support both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) simultaneously. [BP1599]

- Design DNS infrastructure in accordance with appropriate governing IPv6 Transition Office requirements. [BP1705]

- Any Internet Protocol Version 6 (IPv6) address used on DoD systems must be originated at DISA. [BP1600]

- The Domain Name System (DNS) implementation should reflect the guidance provided in Domain Name System Security Technical Implementation Guide. [BP1662]

- Any Domain Name System (DNS) design should be done in coordination with the appropriate governing Internet Protocol Version 6 (IPv6) Transformation Office. [BP1663]

2.2.3 Routers

Routers not only provide the main connection to the Global Information Grid (GIG), but they also are a first line of computer network defense. The devices are complex and proper configuration is essential. In addition to connectivity and routing, they also provide security filtering, address management, network management, and time synchronization. There is a GIG Router Working Group (GRWG) that is addressing implementation issues.

Components should be able to operate in a heterogeneous environment. The presence of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) packets and services in a dual stack environment should not cause a degradation of application performance.

Best Practices

- Routers should be configurable to provide dynamic Internet Protocol (IP) address management using Dynamic Host Configuration Protocol (DHCP). [BP1601]
- Routers should be configurable to provide static Internet Protocol (IP) address. [BP1602]
- Routers should be configured to provide static addresses as defined by the Network Security Technical Implementation Guide (STIG). [BP1603]
- Node routers should be configurable to provide time synchronization services using Network Time Protocol (NTP). [BP1604]
- Node routers should be configurable to provide multicast addressing. [BP1605]
- Node routers should be remotely manageable from within the Node. [BP106]
- Node routers should be configured according to National Security Agency (NSA) Router Configuration guidance. [BP1607]
- Configure routers in accordance with the National Security Agency (NSA) Router Security Configuration Guide. [BP1664]
- Routers should be configured to update the Node’s internal DNS service in accordance with the Network Security Technical Implementation Guide (STIG). [BP1662]
- Routers should be configured in accordance with Network STIG. [BP1699]
- Routers should be configured in accordance with Enclave STIG. [BP1700]

2.2.4 Time Services

Net-centric operations and security depend on synchronized date/time. Many protocols rely upon synchronized time to function properly, particularly security protocols. Mission Component logic and the usefulness of data can also suffer if there is not a common understanding and synchronization of time across the enterprise.

Best Practices

- Node routers should be configurable to provide time synchronization services using Network Time Protocol (NTP). [BP1604]
- Node time service should obtain its reference time from a globally synchronized time source. [BP1608]

- A Node should have a backup time source. [BP1609]

2.2.5 Mobile and Dynamic Networks

Nodes can be mobile or deployable as well as fixed. Mobile networks, by their very nature, are untethered and usually reliant upon Radio Frequency (RF) transmissions. While there are many RF and network engineering challenges regarding the implementation of RF, such communications topics are outside the scope of NESI. The challenge to be addressed herein is that of ensuring uninterrupted Global Information Grid (GIG) interoperability as the underlying network changes dynamically.

Note: Goal of mobile or deployable Nodes are that they can plug into different locations in the GIG without loss of interoperability.

2.2.6 Multicast

Multicast addressing is currently in use in pockets throughout the DoD to support capabilities such as collaboration and alerting, and the use of multicast addressing is growing. Multicast capability is being actively engineering into the Global Information Grid (GIG). Careful planning is still required, however, until multicast becomes ubiquitous across the entire GIG.

Best Practices

- Routers should be configurable to provide dynamic Internet Protocol (IP) address management using Dynamic Host Configuration Protocol (DHCP). [BP1601]

- The Dynamic Host Configuration Protocol (DHCP) services should be configured to assign multicast addresses. [BP1610]

- The Node should anticipate that multicasting will be required even if not used currently and this should be considered in the design of the Node's networks including the selection of Components and Configuration. [BP1706]

2.2.7 Network Information Assurance

Implementation of the DoD Information Assurance (IA) Strategic Plan is required to comply with the DoD Net-Ready Key Performance Parameter (NR-KPP). Components that implement IA, however, can be a barrier to interoperability by default; proper implementation is critical. Furthermore, as net-centric applications and services emerge, so too will the need to dynamically configure the IA Components to permit net-centric operations. As an example, access control based on Internet Protocol (IP) address would not work, as the addresses of service users will not be known *a priori* when such services are dynamically discoverable.

The DoD provides requirements and extensive guidance for the implementation of information assurance at the DISA Information Assurance Support Environment (IASE) Web site. In particular, the Network STIG on the IASE Web site provides guidance for the network implementation, particularly the boundary between the Node's internal network and external networks. It identifies several IA systems, capabilities, and configurations as listed below and provides guidance for implementation of each.

Rather than repeating the contents of specific guidance in this document, readers should check the IASE Web site for current Network IA guidance on topics such as the following:

- External Network Intrusion Detection System (IDS), anomaly detection, or prevention device if required by the Computer Network Defense Service Provider (CNDSP)

- Routers Security with Access Control Lists

- Firewall and application level proxies (may be separate device to proxy applications)

- Internal Network Intrusion Detection (NID) system

- DMZ, if applicable for publicly accessible services

- Split Domain Name Service (DNS) architecture

- Secure devices and operating systems (i.e., STIG compliant)

- Ports and protocols

Furthermore, DoD computer network defense (CND) policies "…mandate all owners of DoD information systems and computer networks enter into a service relationship with a CNDS provider."

Best Practice

- Components should be configured for IA in accordance with Network STIG. [BP1701]

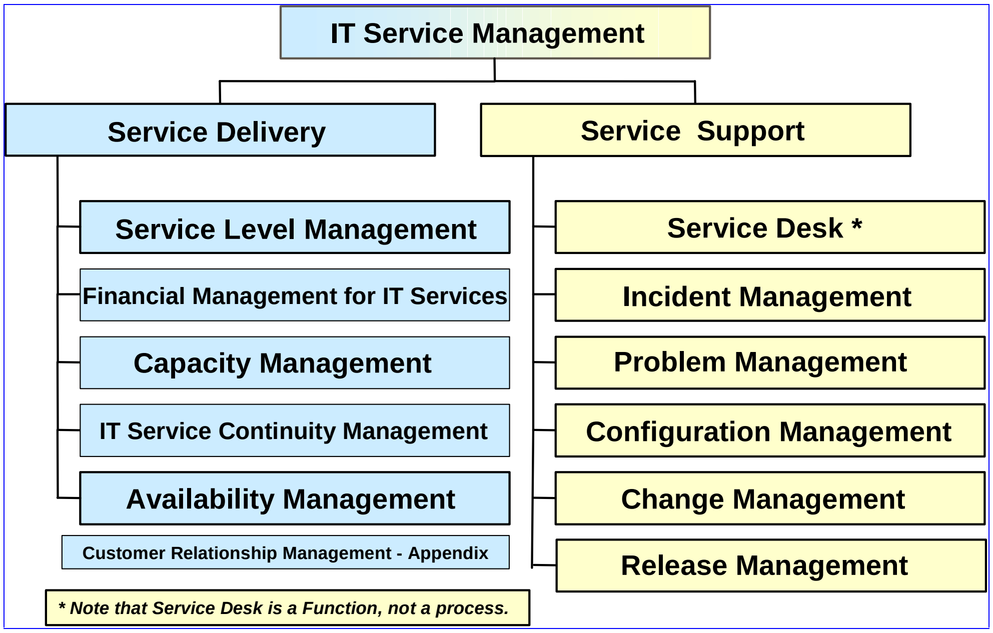
References

- DoD Directive O-8530.1, "Computer Network Defense"

- DoD Instruction O-8530.2, "Support to Computer Network Defense Services (CNDS)"

2.2.8 Enterprise Management Services

Enterprise Management Services (EMS) are fundamental to execution of Service Level Agreements (SLAs), which are inherent in net-centric operations. EMS services are often used internal to a Node using a variety of COTS tools. In a net-centric context, though, EMS must be extended to address inter-nodal service availability and reliability guarantees. Beyond the simpler task of maintaining status information such as link status or service up/down status, EMS must be extended to address complex service arrangement that may involve multiple, orchestrated services. Additionally, coordinated help-desk and reporting will be needed. Some of these topics are being addressed under the DoD NetOps concept.



2.2.9 Virtual Private Networks (VPN)

Virtual Private Networks (VPNs) create a private “tunnel” within a network by encrypting traffic between specified end points. If a VPN is required at a Node, it should be implemented in accordance with the guidance provided in the Network STIG. Services and information intended to be broadly accessible to other Global Information Grid (GIG) Nodes should not be placed behind a VPN because it will be reachable to only the Nodes that are part of in the VPN.

Best Practices

- A Virtual Private Network (VPN) should be implemented in accordance with the guidance provided in the STIG. [BP1667]
- Services and information intended to be broadly accessible to other Nodes should not be placed behind a VPN. [BP1702]

2.2.10 Trusted Guards

Trusted guards are accredited to pass information between two networks at different security levels, such as between SECRET General Service (GENSER) and TOP SECRET Sensitive Compartmented Information (SCI) level networks, according to well defined rules and other controls. Guard products only pass defined types of information (e.g., email, images, or formatted messages). A key challenge is how to implement net-centric operations across trusted guards in the presence of CES services. See the Cross-Domain Interoperation perspective (Section 2.4.1.4) for additional information.

Best Practices

- Nodes should not build Guard Products. [BP1653]
- Components should not build Guard Products. [BP1654]

- Guard products should be acquired and configured with the help of the Government program offices that acquire such guards. [BP1668]

- XML-capable guards should be used, in anticipation that net-centric solutions through guards will rely heavily on the passing of XML messages. [BP1669]

2.2.11 Integration of Non-IP Transports

Systems that are not Internet Protocol (IP) networked, such as aircraft data links (Link-16, SADL, etc.), should implement IP gateways to interoperate with the Global Information Grid (GIG) until IP is supported natively. Most such systems already have plans for transition to IP networking, and gateways are an interim measure.

The gateway should be implemented as a service in accordance with *NESI Part 5: Developer Guidance*. This does not mean that the service would be limited to request/reply or other such usage patterns. In fact, for high-frequency data, such as track reporting, a function of the service could be to set up an out-of-band communication with a subscriber.

Best Practices

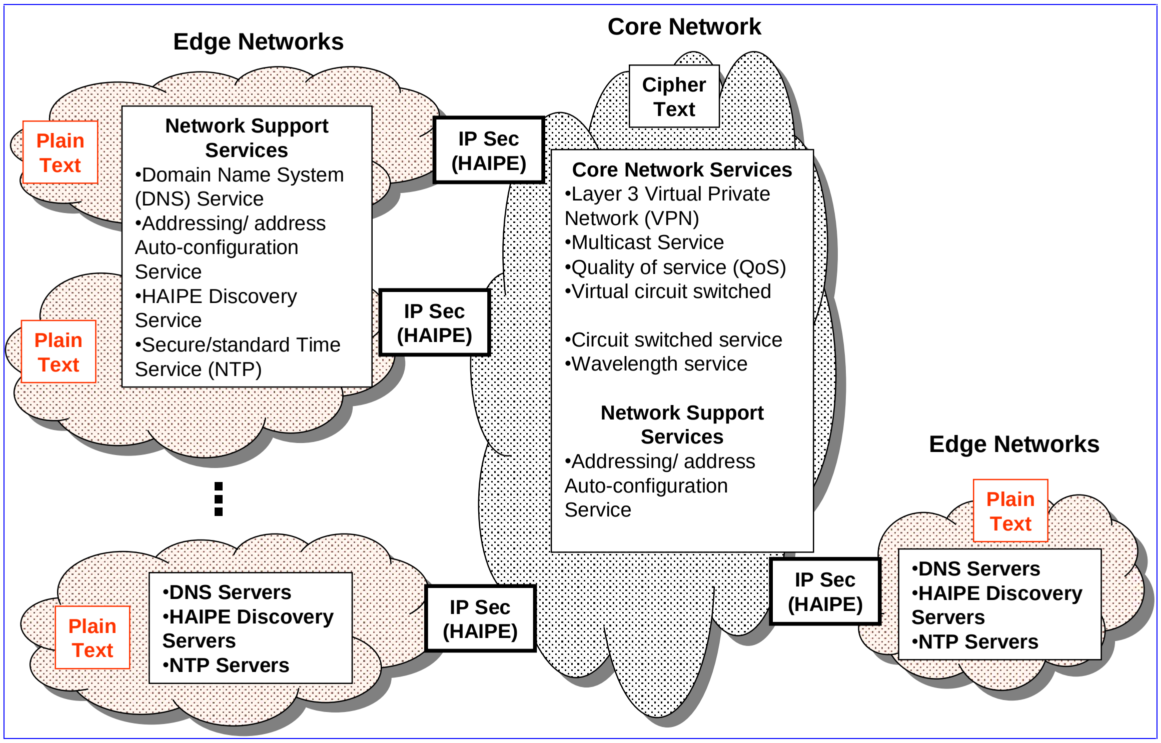
- Components that are not Internet Protocol (IP) networked, such as aircraft data links (Link-16, SADL, etc), should implement IP gateways to interoperate with the Global Information Grid (GIG) until IP is supported natively. [BP1611]

- The gateway should be implemented as a service. [BP1612]

2.2.12 Black Core

The DoD will be aggregating Internet Protocol (IP) packet traffic from multiple security enclaves onto network segments secured at the network layer in the protocol stacks; these segments are called the *Black Core*. This will be enabled through use of High Assurance Internet Protocol Encryption (HAIPE) devices. Challenges to the implementation of HAIPE devices and the Black Core include organic support for the following: IP-based quality of service (QoS), dynamic unicast IP routing, support for dynamic multicast IP routing, support for mobility, and support for simultaneous Internet Protocol Version 6 (IPv6) and Internet Protocol Version 4 (IPv4) operation.

The Black Core is a concept fundamental to Global Information Grid (GIG) networking, but it is listed last in this document because there is little actionable guidance that can be provided at this time. Interoperability with the Black Core will require active monitoring by the Node's management and program offices. The basic architecture of the Black Core is shown in below. The Node typically provides one or more edge networks as shown in the diagram, along with the services indicated. The edge (Node) networks are sometimes referred to as Plain Text (PT) networks, while the Black Core is the Cipher Text (CT) network.



Best Practices

- Black Core implementation issues should be monitored by the Node and a plan prepared for local implementation in coordination with system programs fielded within the Node. [BP1670]

- Black Core transition should be considered whenever there is a significant Node network design or configuration decision to make, in an effort to avoid costly downstream changes caused by Black Core transition. [BP1671]

2.3 Node Computing Infrastructure

There are several elements of the computing infrastructure having significant effect on Global Information Grid (GIG) interoperability. Other elements of the computing infrastructure, such as Host Management, Backup/Restore, and Software/Patch Distribution are outside the scope of NESI because they have little impact on net-centricity or interoperability across GIG Nodes. The following elements have a direct bearing on net-centricity or interoperability:

- Web Client Platform
- Web Application Infrastructure
- Host Information Assurance
- Domain Directories
- Instrumentation and Metrics

2.3.1 Web Client Platform

Web clients (both desktops and servers) should be capable of accessing Java Platform, Enterprise Edition (Java EE) services and .NET services; service developers are free to choose the best technology for their service.

Two key elements of the standard frameworks follow:

- Browser
- CAC Reader

Best Practices

- A Node should be prepared to host new Component services developed by other Nodes or by the enterprise itself. [BP1613]

- A Node should be prepared to become new Component service within another Node. [BP1614]

- The Node should be prepared to fully integration with the Information Assurance (IA) infrastructure. [BP1672]

- The Node should be prepared to fully integration with the Enterprise Management Services (EMS) infrastructure. [BP1673]

2.3.1.1 Browser

Web browsers are fundamental to the DoD vision of net-centric information sharing and access to distributed services. Because Global Information Grid (GIG) interoperability partners may not be known *a priori*, Web browsers should support a wide breadth of browser technologies, such as JavaScript, Java applets, and plug-ins.

The browser should be configured in accordance with the Web Server Technical Implementation Guide (STIG), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG.

Best Practices

- Web browsers should support a wide breadth of browser technologies that can be used to extend the browsers' functionality. [BP1615]

- The browser should be configured in accordance with the Web Server Technical Implementation Guide (STIG), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG. [BP1674]

2.3.1.2 Common Access Card (CAC) Reader

Smart cards provide greatly increased security for multiple applications. The usefulness of a smart card is based on its intrinsic portability and security. A typical smart card has the same dimensions as a standard credit card and appears to be very similar with the exception of a set of gold contacts. When inserted into a reader, these contacts provide power to a microprocessor located on the smart card; the smart card is thus able to store and process information, in particular cryptographic keys and algorithms for providing digital signatures and for use with other encryption. A major impediment to the widespread use of smart cards has been interoperability. Unfortunately, smart cards are currently not vendor interoperable and therefore must use specific software and smart card readers. This is an issue that is being addressed by the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL).

Best Practices

- A server should be configured with a Common Access Card (CAC) reader [BP1618]

- A client should be configured with a Common Access Card (CAC) reader [BP1619]

Reference

- DoD Common Access Card

2.3.2 Web Infrastructure

A Web infrastructure allows software developers to deploy Web-enabled applications, services and other software in a Node. While many Web infrastructures exist, most software will converge on one or two popular platforms or technologies (e.g., Apache, Java Enterprise Edition, .NET, etc.). The Node should provide common shared Web infrastructures for software deployments to minimize unnecessary duplication of these common environments. A common Web infrastructure will also allow Nodes to better provide full integration with local Information Assurance (IA) and Enterprise Management Services (EMS) infrastructures as well as CES and COI services available both internally and externally to the Node.

There are three major elements to Web infrastructure that need to be addressed at the Node:

- Web Portal
- Web Server
- Web Application Containers

Best Practices

- The Node's Web infrastructure should be accessible and used by all the Components that are hosted at the Node. [BP1621]

- The Web infrastructure should support the technologies and standards used by the CES services under development as well as any technologies and standards used for Community of Interest (COI) services. [BP1675]

- Configure and locate elements of the Node Web infrastructure in accordance with the Web Server STIG. [BP1707]

- Configure and locate elements of the Node Web infrastructure in accordance with the Desktop Applications STIG. [BP1708]

- Configure and locate elements of the Node Web infrastructure in accordance with the Network STIG. [BP1709]

- Nodes should consider using Web proxy servers and load balancers. [BP1677]

2.3.2.1 Web Portal

A Web portal provides an environment for hosting small Web applications called portlets, and allows for content selection, arrangement and other visual preferences tailored to each user. Though not strictly essential for Global Information Grid (GIG) interoperability, it can reasonably be expected that some GIG net-centric services and applications will provide portal based Web applications that Nodes may want to host locally. To reduce issues of portability, Web portals provided by the Node should support widely accepted standards such as JSR-168 and Web Services for Remote Portlets (WSRP). However, because commercial products also provide non-portable proprietary interfaces, there is a risk that multiple Web portal products may be required or that the portlet would have to be reengineered to work on an existing Node portal. (See the Web Portals perspective in *NESI Part 5: Developer Guidance* for additional information).

Best Practice

- Support appropriate and widely accepted standards for Web portals provided by the Node [BP1710]

2.3.2.2 Web Server

Web server technology is becoming fundamental in making information visible and accessible to external Global Information Grid (GIG) users. The most significant barrier to interoperation is security. Making information accessible to a community of users as large as the GIG necessitates the implementation of authentication and authorization technology that is sufficient to prove a user's identity and that is scalable, respectively. Web servers should provide DoD Public Key Infrastructure (PKI) based authentication and role based authorization mapped to certificate attributes as described in the applicable STIGs. Eventually, the container should integrate with the Net-Centric Enterprise Services (NCES) Security Service, when available. In the interim, authorization should be based on the Electronic Data Interchange – Personnel Identifier (EDI-PI) contained in the PKI certificate attributes. The use of the EDI-PI as the attribute on which to base authorization decisions is a matter of debate and ongoing engineering, as there are issues about the issuance of EDI-PI to certain user populations, such as coalition users. In the absence of an EDI-PI attribute, other attributes should be used for authorization decisions. (For additional technical level guidance on Web servers, see *NESI Part 5: Developer Guidance*.)

2.3.2.3 Web Application Containers

Web application containers provide an environment for serving full, interactive application functionality and services on the Web. There are two major container technologies: Java Platform, Enterprise Edition (Java EE) and .NET. NESI expresses no preference regarding which of the two technologies is used; *NESI Part 5: Developer Guidance* addresses both.

The design and implementation of a Node's Web infrastructure should accommodate both Java EE and .NET. The rationale for this is that Nodes will likely have to host services locally and applications that were developed externally using either technology. Web services (Simple Object Access Protocol or SOAP, XML, etc.) should be used to interoperate between Java EE and .NET applications or services. Such interoperation may be required, for example, when orchestrating Web services across Nodes as part of a Joint mission thread.

As was the case with Web servers, application containers should provide DoD Public Key Infrastructure (PKI) based authentication and role based authorization mapped to certificate attributes as described in the applicable STIGs. Eventually, the container should integrate with the Net-Centric Enterprise Services (NCES) Security Service, described in Section 8.2.2, when available. In the interim, authorization should be based on the Electronic Data Interchange – Personnel Identifier (EDI-PI) contained in the PKI certificate attributes. The use of the EDI-PI as the attribute on which to base authorization decisions is a matter of debate and ongoing engineering, as there are issues about the issuance of EDI-PI to certain user populations, such as coalition users. In the absence of an EDI-PI attribute, other attributes should be used for authorization decisions.

The Web application container should be capable of processing Web services protocols in accordance with the Web Services Interoperability (WS-I) Basic Profile. The container should also support XML security protocols including XML Encryption, XML Signature, and XML Key Management. These protocols are used in protecting content within an XML document that may be passed amongst multiple Web services that are orchestrated. Specific development guidance on the development of services on Web application containers is provided in *NESI Part 5: Developer Guidance*.

2.3.3 Host Information Assurance

Host Information Assurance (IA) protections are part of the DoD Information Assurance Strategic Plan, which in turn is a part of the Net-Ready Key Performance Parameter (NR-KPP) that gets assessed during the Joint Capabilities Integration and Development System (JCIDS) acquisition process. Failure to implement host information assurance protections could jeopardize the approval for a Node to operate on the Global Information Grid (GIG).

Best Practices

- Commercial off-the-shelf (COTS) virus scanning and worm detection software, along with accompanying capabilities for update of software and virus definitions, should be implemented on each client or server hardware in accordance with the Desktop Applications STIG. [BP1622]

- Personal firewall software should be implemented on client or server hardware used for remote connectivity, in accordance with the Desktop Applications STIG, Network STIG, and Enclave STIG. [BP1623]

- Anti-spyware must be installed on all client and server hardware. [BP1624]

2.3.4 Domain Directories

Within and across Nodes, directory technologies such as Microsoft's Active Directory (AD) or OpenLDAP are used as tools for system, network, and security administration. Many options exist on how Nodes employ these tools; however, interoperability issues can arise between Global Information Grid (GIG) Nodes if sub-enterprises employ these tools differently (even within the same technology family, such as AD).

Guidance on Active Directory implementation is being formed by the DoD Active Directory Interoperability Working Group (DADIWG).

Active Directory (AD), if used, should be implemented in accordance with the recommendations of the DADIWG. The DADIWG Web Site prior should also be periodically monitored for the status of GIG implementation issues.

Best Practice

- A Node that uses Active Directory (AD) should be implemented in accordance with the recommendations of the DoD Active Directory Interoperability Working Group (DADIWG). [BP1679]

2.3.5 Instrumentation for Metrics

Performance has an impact on net-centric operations. Instrumentation is a term frequently used in association with the generation, collection, and analysis of performance metrics. In a dynamic environment, where services and information exchange partners may be dynamic, metrics can be a key factor in the selection of services. Performance metrics that are advertised externally and frequently updated allow potential service users the ability to select an implementation that meets their performance requirements, such as a measurement of reliability. Metrics are normally also needed to ensure performance is provided according to more traditional Service Level Agreements (SLAs), and for operations management.

Component services that are exposed to the Global Information Grid (GIG) by a Node should be instrumented to collect performance metrics. Metrics should be visible and accessible as part of the Component service registration and updated periodically. Standards for metrics are not defined by expected at some point in the future by appropriate GIG working groups.

Some draft metrics that may be appropriate for Web services are given in the following table:

SLA Metric	Metric Description
Availability	How often is the service available for consumption?
Accessibility	How capable is the service of serving a client request now?
Performance	How long does it take for the service to respond?
Compliance	How fully does the service comply with stated standards?
Security	How safe and secure is it to interact with this service?
Energy Efficiency	How energy-efficient is this service for mobile applications?
Reliability	How often does the service fail to maintain its overall service quality?

Best Practices

- Component services that are exposed to the Global Information Grid (GIG) by a Node should be instrumented to collect performance metrics. [BP1680]

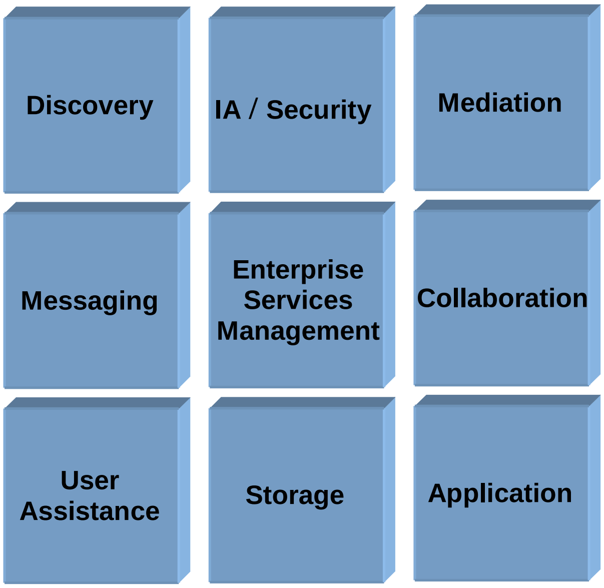
- Component services metrics should be visible and accessible as part of the service registration and updated periodically. [BP1681]

2.4 Node Application Enterprise Services

The DoD has developed an Enterprise Services Strategy that obligates Nodes to employ Enterprise Services to achieve net-centric information sharing. The ultimate goal is to connect people or systems that need information with people or systems that have information. In the strategy, information is considered to be data and/or services. The connection between the information providers and information consumers is the through the use of core enterprise capabilities. Within the DoD, DISA has been chartered to define and develop these capabilities through a project called Net-Centric Enterprise Services (NCES). NCES has the following vision:

> *NCES will enable the secure, agile, robust, dependable, interoperable data-sharing environment for DoD where warfighter, business, and intelligence users share knowledge on a global network that facilitates information superiority, and accelerates decision-making, effective operations, and net-centric transformation.*

In order to accomplish this interconnectivity, NCES has identified nine capabilities that are mapped to services. Collectively, these services are called the Core Enterprise Services (CESs).


Discovery
IA / Security
Mediation
Messaging
Enterprise Services Management
Collaboration
User Assistance
Storage
Application

Discovery Search, locate or publish data (content), other capabilities (services), or users across the Global Information Grid (GIG).

IA/Security Authorizes and authenticates Global Information Grid (GIG) users to ensure the confidentiality and integrity of information and services.

Mediation Translates, brokers, aggregates, fuses or integrates data into commonly understood formats.

Messaging Distributed, machine-to-machine messaging for notifications and alerts.

Enterprise Service Management Monitor/manage Global Information Grid (GIG) Enterprise Services against operational performance parameters to ensure reliability and availability of critical capabilities.

Collaboration Allows users to work together securely on the network by way of video, audio, text chat, white boarding, online meetings, work groups, application sharing.

User Assistance Provides automated "helper" capabilities and user preferences to help maximize user efficiency in task performance.

Storage Provides physical and virtual places to host and retain data for purposes such as content staging, continuity of operations, or archival.

Application Provides the resources necessary to provision, operate and maintain Net-Centric Enterprise Services (NCES) capabilities.

The nine CES are being developed for the entire GIG enterprise by NCES. NCES is using a Software Product Line (SPL) approach to facilitate the building of the CES. The Software Engineering Institute (SEI) defines SPL as follows:

> *A software product line (SPL) is a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way. Software Engineering Institute*

NCES has divided the problem into four product lines:

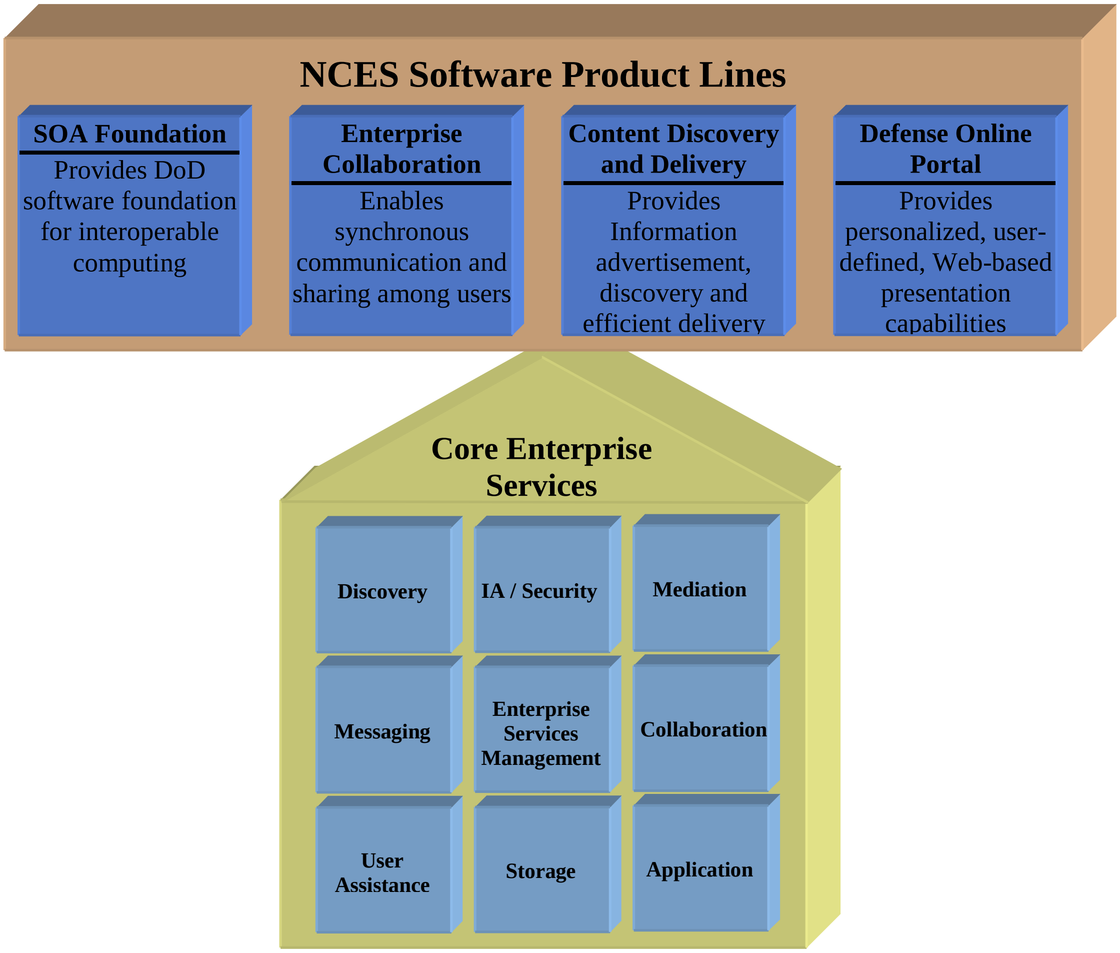
SOA Foundation Provides the DoD software foundation for interoperable computing

Enterprise Collaboration Enables synchronous communication and sharing among users.

Content Discovery and Delivery Provides Information advertisement, discovery and efficient delivery

Defense Online Portal Provides personalized, user-defined, Web-based presentation capabilities.

The CES services will be provisioned by DISA and operated on the Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) global networks, initially operating from DISA Enterprise Computing Centers (DECCs).


NCES Software Product Lines
SOA Foundation
Provides DoD software foundation for interoperable computing
Enterprise Collaboration
Enables synchronous communication and sharing among users
Content Discovery and Delivery
Provides Information advertisement, discovery and efficient delivery
Defense Online Portal
Provides personalized, user-defined, Web-based presentation capabilities
Core Enterprise Services
Discovery
IA / Security
Mediation
Messaging
Enterprise Services Management
Collaboration
User Assistance
Storage
Application

The CES and SPL approach is very flexible. As a consequence, the exact mechanism of how CES services are employed by Nodes is a topic of active discussions. Overarching issues include maturity, availability, disconnected operations, cross-domain security, and compliance, as described briefly below.

- Overarching Issues
- Core Enterprise Services (CES)
- Community of Interest (COI) Services

2.4.1 Overarching Issues

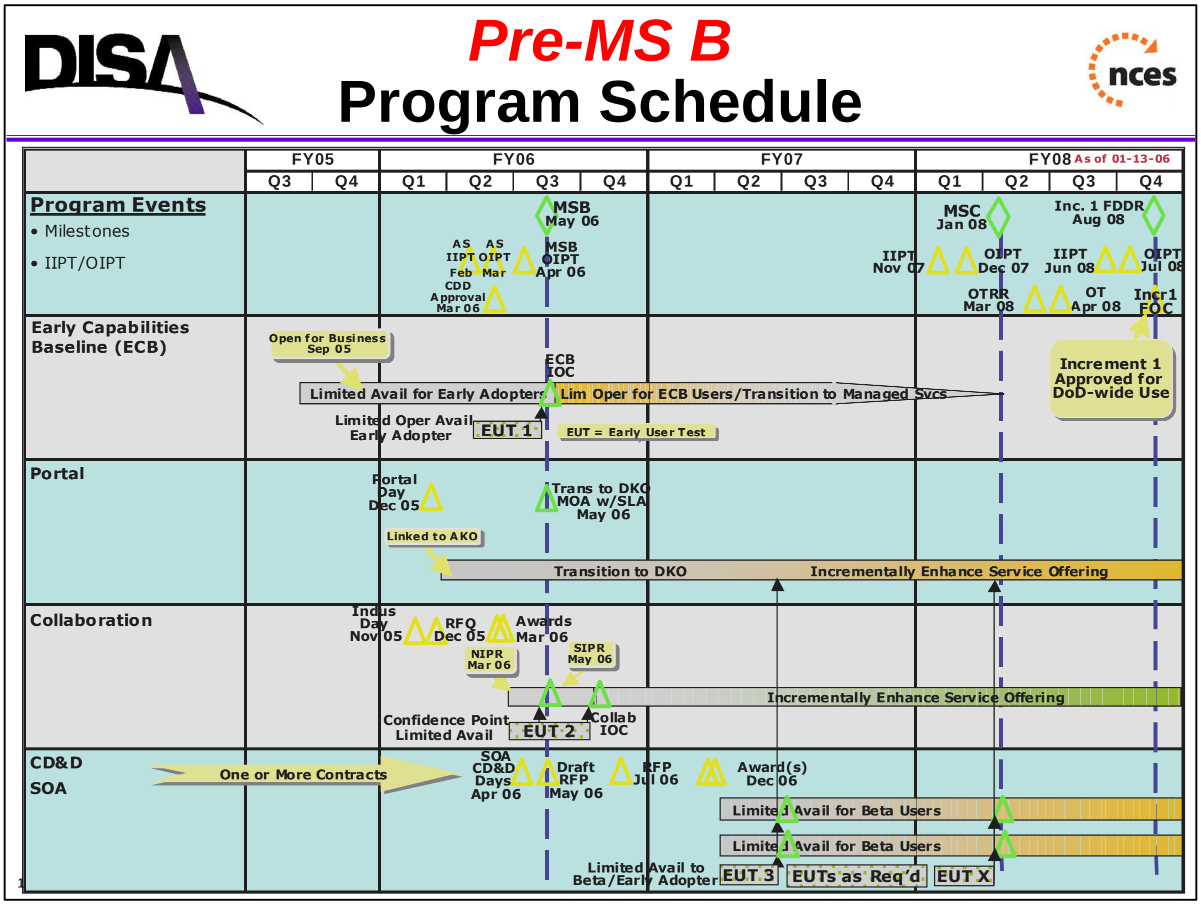
Overarching issues include maturity, availability, disconnected operations, cross-domain security, and compliance. Overarching issues have been divided into the following elements:

- CES Definitions and Status
- CES Parallel Development
- CES and Intermittent Accessibility
- Cross-Domain Interoperation
- Key Interface Profile (KIP) Compliance
- Net-Ready Key Performance Parameter (NR-KPP)

- Core Enterprise Services (CES)

2.4.1.1 CES Definitions and Status

The CES capabilities are in various states of maturity. The Net-Centric Enterprise Services (NCES) program is currently scheduled for a Milestone B decision in the third quarter of 2006.



Pre-MS B
Program Schedule

Capabilities will be delivered in increments; CES Increment 1 capabilities, shown below, are scheduled for operation beginning in 2008 (source: https://ges.dod.mil/soa.htm).

Service Discovery Provides a "yellow pages," categorized by DOD function, enabling users to advertise and locate capabilities available on the network.

Service Security Provides a layer of defense in depth that enables protection, defense, and integrity of the information environment.

Identity Management Provides the methodology and functions for maintaining information on people, consumers, and service providers. Supports the validation of identity authentication credentials.

Service Management Enables monitoring of DOD Web services. Provides reporting of service-level information to potential and current service consumers, program analysts, and program managers.

Service Mediation Allows disparate applications to work together across the enterprise by supporting the transformation of information from one format to another, and the correlation and fusion of data from diverse sources. Supports creation and implementation of process workflows across the enterprise.

Machine-to-Machine Messaging Provides reliable machine-to-machine message exchange across the enterprise.

Metadata Services Provides access to Extensible Markup Language (XML) data elements, taxonomy galleries, schemas, and validation and generation tools for DOD software developers.

DOD Web Services Profile Provides specifications and implementation guidelines to maximize interoperability across DOD Web service implementations.

NCES Increments will be rolled out every 24-26 months. The NCES increment schedule should be considered in scheduling Node evolution, in coordination with systems within the Node.

Best Practices

- A Node should provide an environment to support the development, build, integration, and test of net-centric capabilities by its Components. [BP1576]

- Identify which Core Enterprise Services (CES) capabilities the Node Components require. [BP1626]

- Identify the priority of each Core Enterprise Services (CES) capabilities the Node Components require. [BP1627]

- Identify which Net-Centric Enterprise Services (NCES) capabilities the Node requires. [BP1628]

- Identify which Net-Centric Enterprise Services (NCES) capabilities the Node requires during deployment. [BP1629]

- Coordinate Node schedule with the Net-Centric Enterprise Services (NCES) schedule. [BP1683]

- Coordinate the Node schedule with the Component schedules. [BP1684]

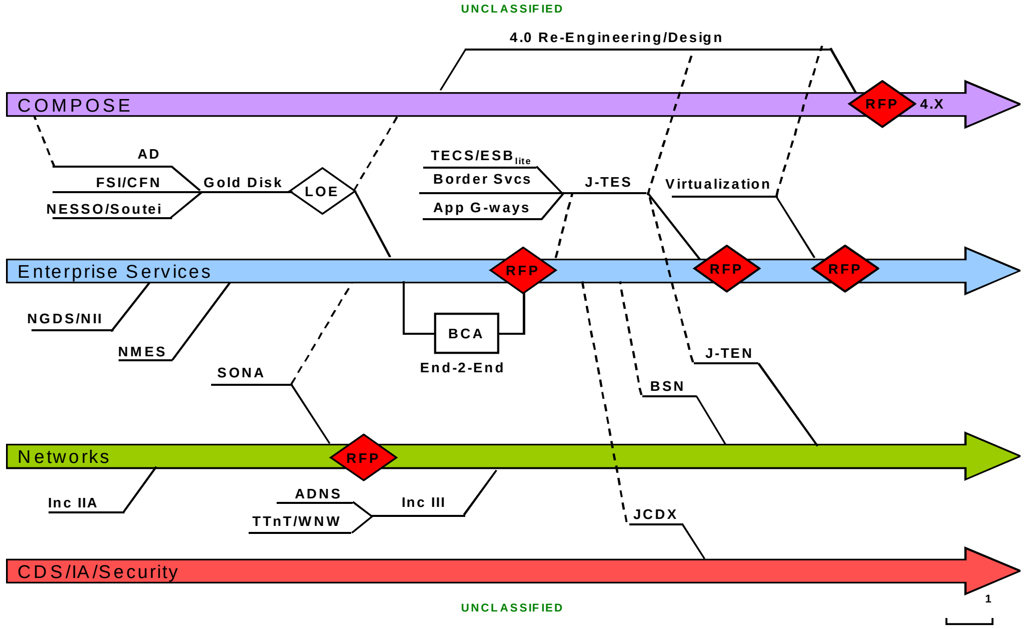
- Mobile Nodes that rely on Transmission Control Protocol/Internet Protocol (TCP/IP) for inter-node communication should engage with the Net-Centric Enterprise Services

(NCES) program office to explore approaches for mobile use of the Core Enterprise Services (CES) services. [BP1661]

- The Web infrastructure should support the technologies and standards used by the Core Enterprise Services (CES) services under development, as well as any technologies and standards used for Community of Interest (COI) services. [BP1675]

Example

The following is an example of how a Service-Oriented Architecture (SOA) Roadmap could be developed by the Navy PEO C4I & Space Networks, IA and Enterprise Services Program Management Office (PMW160) for a project called COMPOSE. The Roadmap lays out the deliveries for four layers: COMPOSE itself, Enterprise Services, Networks, and Security. The milestones and the availability and interdependences of the various parts are documented.



2.4.1.2 CES Parallel Development

Availability of the CES services will be a continuing challenge until all services reach full maturity and operational status. The following table is taken from the Net-Centric Enterprise Services (NCES) workspace of the Defense Online Web site and shows the availability of services comprising the NCES Discovery capability. Designating a CES liaison should help to monitor the availability of CES functionality and report on them back through the engineering processes of the Node and Components within the Node. Conversely, the engineering processes for the Node and Components should specifically include provisions for incremental implementation of the CES services.

To accelerate the maturation and implementation of the CES, DISA established an *Early Adopter* process. Early adopters can participate in service pilots, as described in the Pilot Participant’s Guide (draft).

Use the early adopter process and service pilots to accelerate implementation of the CES within the Node. Many factors influence the decision to participate in the early adopter process and pilots including acquisition phase, funding, mission, and priorities for individual systems as well as the aggregate Node. Develop a Node-specific service implementation plan.

Nodes operating at special classification levels should coordinate with other Nodes within the same level and with DISA to host CES services on the relevant networks.

Best Practices

- Nodes should specifically include provisions for incremental implementation of the CES services. [BP1649]
- Components should specifically include provisions for incremental implementation of the hosting Node's CES services. [BP1650]
- Nodes should define an enterprise service schedule for interim and final enterprise capabilities. [BP1577]
- Components should define a schedule that covers the use of the Enterprise Services defined within the Node's enterprise service schedule. [BP1578]
- Identify the priority of each Core Enterprise Services (CES) capabilities are required by the Node's Components. [BP1627]
- Nodes must coordinate with other Nodes having the same compartmentalization needs and DISA to host compartmentalization CES. [BP1694]
- Coordinate Node's schedule to Net-Centric Enterprise Services (NCES) schedule. [BP1684]
- Coordinate Node's schedule to Component's schedule. [BP1684]
- A CES liaison should be designated to monitor the availability of services. [BP1695]
- The Early Adopter process and service pilots should be used to accelerate implementation of the CES services within the Node. [BP1696]
- The parallel development of CES outside the control of the Node should be a part of the risk management activities. [BP1697]

2.4.1.3 CES and Intermittent Availability

There are two related challenges: how to handle lapses in the availability of CES services and how to align inter-Node and intra-Node solutions. CES services may be unavailable for several reasons, including loss of connectivity, actual service unavailability, or service rejection. The lack of availability of CES services must not disrupt intra-node availability of locally hosted services. While alignment of intra- and inter-node technical solutions is very desirable, the interface to locally hosted Components must not be dependent on the availability of CES services.

Specific guidance is largely dependent upon the specific Node operating environment and mission. There appear to be some basic options for meeting these challenges:

- Locally host failover copies of certain CES services. Components that are dependent upon Enterprise Services for infrastructure functions, such as security, continue to operate after failing over to the local instances until enterprise accessibility is re-established. This approach requires replication of enterprise services data (the data used by the enterprise services) between the local failover services and the “master” enterprise services. It also requires development of failover behavior in the applications, services, and infrastructure.

- Develop Components to be adaptive, applying default rules and behaviors when Enterprise Services are inaccessible. This approach, along with the definition of the default rules and behaviors would depend on factors such as the sensitivity and importance of the information involved. For example, access control decisions might default to local capabilities such as Active Directory local user accounts. Or local caching might be used to retain the most recently known values for information such as previously discovered services.

- Employ separate external-facing and internal-facing implementations of published services so that external disruptions do not affect local accessibility. The external-facing copy of the service could use Enterprise Services, and the internal-facing copy could implement local Node behavior. As an example, the external-facing copy could implement Public Key Infrastructure (PKI) authentication and authorization, whereas the internal-facing copy could implement Active Directory security. The challenge in this approach is in the coordination of the external-facing and internal-facing copies of such services, such as to provide shared access to databases or replication of data between the external-facing and internal-facing implementations.

Nodes and Components will likely employ some combination of, or evolution of, the above options.

Uniformity and alignment between the technical mechanisms for accessing local services and Enterprise Services should be an objective. Where possible, the burden of providing such uniformity and alignment should rest on the Node infrastructure, rather than the individual Components within the Node, thus isolating the complexities and making them more manageable. Consider the necessity of using CES-provided SDKs and Key Interface Profile (KIP) compliance when formulating an approach; use of an approved SDK may drive separation of external-facing and internal-facing implementation described in the last option above. Finally, the immaturity of the CES services and the alignment of local and external services access, as a whole, should figure prominently in the risk management activities of the Node and Components within the Node.

Best Practices

- Node implemented CES should comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1630]

- Node services proxies should expose CES that comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1631]

- Components should not implement server side CES functionality. [BP1651]

2.4.1.4 Cross-Domain Interoperation

By and large, the implementation of net-centric concepts across security domains has not been defined. Trusted guards do not act as network routers; information to be transferred across a guard is delivered to the guard, processed, and then delivered to a defined endpoint on the other side if the rules are satisfied. The guard in the middle disrupts the normal pattern for use of the CES services.

In order for services to work through the trusted guards that interconnect different domains, there must be a well defined set of messages that can be passed through the guard to effect the conversation necessary to use the service and return results. This restriction, if built into the service's interface, could be unduly restrictive on the design of the interface.

It may be more practical for each such service to provide service proxies for use in the other security domains, and corresponding client proxies in the local domain. The server proxy and client proxy for the service might then communicate across the trusted guard in a private, high efficiency manner that the guard can process. But even this approach is restrictive in that the server proxies have to be installed in the other security domains, and this departs from some fundamentals of net-centric concepts such as dynamic service discovery.

Until such approaches are prototyped and explored more fully, Nodes should anticipate that services will not be capable of cross-domain invocation. Furthermore, for services that have utility in other security domains, implementer should consider providing copies of such services for hosting in the other domains, and use XML document transfers across the trusted guard to keep the copies in synchronization. This approach depends on many factors, and may not be suitable for all services.

Best Practices

- A Node should be prepared to host new Component services developed by other Nodes or by the enterprise itself. [BP1613]

- A Node should be prepared to become new Component service within another Node. [BP1614]

- Node implemented Service Discovery (SD) should be implemented to meet compartmentalization needs. [BP1619]

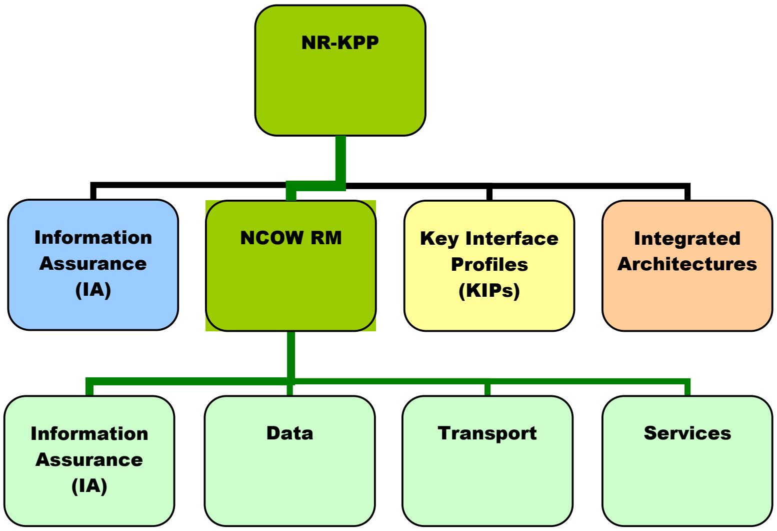
- Nodes should not expect cross-domain invocation of Component's services. [BP1698]

2.4.1.5 Net-Ready Key Performance Parameter (NR-KPP)

The following information is from the Defense Acquisition University (DAU) Defense Acquisition Guidebook, Chapter 7.3.4. The Net-Ready Key Performance Parameter (NR-KPP) has been developed to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving Information Technology (IT) and National Security Systems (NSS) interoperability and supportability. The NR-KPP assists Program Managers, the test community, and Milestone Decision Authorities in assessing and evaluating IT and NSS interoperability.

The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. Program managers will use the NR-KPP documented in Capability Development Documents (CDD) and Capability Production Documents (CPD) to analyze, identify, and describe IT and NSS interoperability needs in the Information Support Plan (ISP) and in the test strategies in the Test and Evaluation Master Plan.

The following diagram explains the relationships of the Global Information Grid (GIG) Key Interface Profiles (KIPs), Net-Centric Operations and Warfare Reference Model (NCOW RM), ASD(NII) Net-Centric Checklist, and the Net-Ready Key Performance Parameter (NR-KPP).


NR-KPP
Information Assurance (IA)
NCOW RM
Key Interface Profiles (KIPs)
Integrated Architectures
Information Assurance (IA)
Data
Transport
Services

- Information Assurance (IA)
- Net-Centric Operations and Warfare Reference Model (NCOW RM)
- Key Interface Profile (KIP)
- Integrated Architectures

References

- See the following items from the Defense Acquisition Guidebook:
  - Compliance with the Net-Centric Operations and Warfare Reference Model
  - Compliance with applicable Global Information Grid Key Interface Profiles
  - Compliance with DoD Information Assurance requirements
  - Supporting integrated architecture products

2.4.1.6 Information Assurance (IA)

Most Nodes delivering capability to the warfighter or business domains will use Information Technology (IT) to enable or deliver that capability. For those Nodes, developing a comprehensive and effective approach to IA is a fundamental requirement and are key in successfully achieving Node's objectives. The DoD defines IA as follows:

> *Information Assurance (IA) are the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.*

DoD policy and implementing instructions on information assurance are in the 8500 series of DoD publications. Nodes and Components for programs should be familiar with statutory and regulatory requirements governing information assurance, and understand the major tasks involved in developing an IA organization, defining IA requirements, incorporating IA in the Node's and Component architecture, developing an acquisition IA strategy (when required), conducting appropriate IA testing, and achieving IA certification and accreditation for the program.

Best Practices

- Nodes should be DoD Information Assurance (IA) certified and accredited. [BP1632]
- Nodes are responsible for only hosting DoD Information Assurance (IA) certified and accredited Components. [BP1633]
- Components should be DoD Information Assurance (IA) certified and accredited. [BP1634]

References

- DoD Directive 5000.1, Enclosure 1, Paragraph E1.9, Information Assurance

  Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in DoD Directive 8500.1....

- DoD Instruction 5000.2, Enclosure 4, Paragraph E.4.2, IT System Procedures states, "The program defines the requirement for an Information Assurance Strategy for Mission Critical and Mission Essential IT systems."

  The DoD CIO must certify (for MAIS programs) and confirm (for MDAPs) that the program is being developed in accordance with the CCA before Milestone approval. One of the key elements of this certification or confirmation is the DoD CIO's determination that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.

- DoD Instruction 5000.2, Enclosure 4, Table E4.T1, CCA Compliance Table: requires that "[t]he program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.
- DoD Directive 8500.1, "Information Assurance (IA)": This directive establishes policy and assigns responsibilities under 10 U.S.C. 2224 to achieve Department of Defense information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to net-centric warfare.
- DoD Instruction 8500.2, "Information Assurance (IA) Implementation": This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.1.
- DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System": This instruction implements policy, assigns responsibilities, and prescribes procedures necessary to integrate Information Assurance (IA) into the Defense Acquisition System; describes required and recommended levels of IA activities relative to the acquisition of systems and services; describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.
- DoD Instruction 5200.40, "DoD Information Technology Security Certification And Accreditation Process (DITSCAP)": This instruction implements policy, assigns responsibilities and prescribes procedures under DoD Directive 8500.1 for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in the DoD.
    - According to DoD Directive 8500.1, all acquisitions of Automated Information Systems (AISs), to include Automated Information System applications, outsourced IT-based processes, and platforms or weapon systems with connections to the Global Information Grid (GIG) must be certified and accredited according to DoD Instruction 5200.40, DITSCAP.
    - See other applicable Certification & Accreditation processes (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information within Information Systems" for systems processing Sensitive Compartmented Information).

2.4.1.7 Net-Centric Operations and Warfare Reference Model (NCOW RM)

The Net-Centric Operations and Warfare Reference Model (NCOW RM) represents the strategies for transforming the enterprise information environment of the Department. It is an architecture-based description of activities, services, technologies, and concepts that enable a net-centric enterprise information environment for warfighting, business, and management operations throughout the Department of Defense. Included in this description are the activities and services required to establish, use, operate, and manage this net-centric enterprise information environment. Major activity blocks include the generic user-interface (A1), the intelligent-assistant capabilities (A2), the net-centric service (core, Community of Interest, and enterprise control) capabilities (A3), the dynamically allocated communications, computing, and storage media resources (A4), and the enterprise information environment management components (A5). Also included is a description of a selected set of key standards and/or emerging technologies that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized.

Transforming to a net-centric environment requires achieving four key attributes: reach, richness, agility, and assurance. The initial elements for achieving these attributes include the Net-Centric Enterprise Services (NCES) Strategy, the DoD Net-Centric Data Strategy, and the DoD Information Assurance (IA) Strategy to share information and capabilities. The NCOW RM incorporates (or will incorporate) these strategies as well as any net-centric results produced by the Department's Horizontal Fusion (HF) pilot portfolio.

The NCOW RM provides the means and mechanisms for acquisition program managers to describe their transition from the current environment (described in GIG Architecture Version 1) to the future environment (described in GIG Architecture Version 2). In addition, the NCOW RM will be a key tool during program oversight reviews for examining integrated architectures to determine the degree of net-centricity a program possesses and the degree to which a program can evolve to increased net-centricity. Compliance with the NCOW RM is one of the four elements that comprise the Net-Ready Key Performance Parameter (NR-KPP).

Best Practice

- Nodes should comply with the Net-Centric Operations and Warfare Reference Model (NCOW RM). [BP1636]

2.4.1.8 Key Interface Profile (KIP)

The following information is from the Defense Acquisition University (DAU) Defense Acquisition Guidebook, Chapter 7.3.4.2. A Key Interface Profile (KIP) is the set of documentation produced as a result of interface analysis which designates an interface as key; analyzes it to understand its architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Systems Engineering Plan, Configuration Management Plan, Technical Standards View (TV-1) with SV-TV Bridge, and procedures for standards conformance and interoperability testing. Relevant Global Information Grid (GIG) KIPs, for a given capability, are documented in the Capability Development Document and Capability Production Document. Compliance with identified GIG KIPs are analyzed during the development of the Information Support Plan (ISP) and Test and Evaluation Master Plan, and assessed during Defense Information Systems Agency Joint Interoperability Test Command (JITC) joint interoperability certification testing. An interface is designated as a key interface when one or more the following criteria are met:

- The interface spans organizational boundaries.

- The interface is mission critical.
- The interface is difficult or complex to manage.
- There are capability, interoperability, or efficiency issues associated with the interface.
- The interface impacts multiple acquisition programs.

Program manager compliance with applicable GIG KIPs is demonstrated through inspection of Joint Capabilities Integration and Development System (JCIDS) documentation and test plans, and during JITC interoperability certification testing (see references [j] and [l], CJCS Instruction 3170.01 and CJCS Instruction 6212.01, respectively, for detailed discussions of the process).

KIPs are being defined to specify the interfaces to the Core Enterprise Services (CES). Compliance with these KIPs is a mandatory element of the Net-Ready Key Performance Parameter (NR-KPP). The KIP specifications are in various states of maturity and may be viewed at http://kips.disa.mil (user registration required).

Best Practices

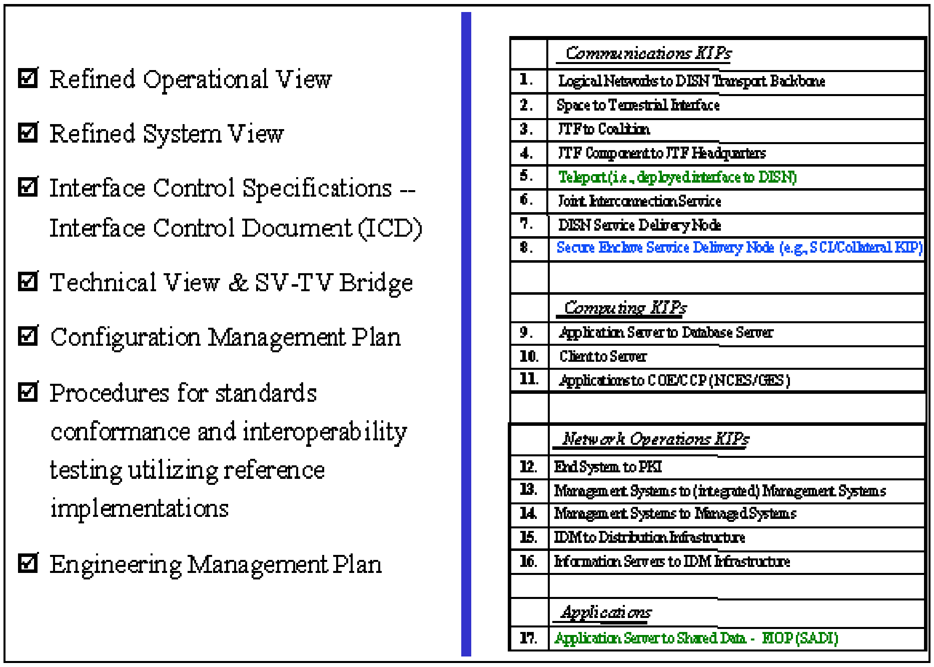
- Node implemented CES should comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1630]

- Node services proxies should expose CES that comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1631]

- For Key Interface Profile (KIP) specifications that are not available or insufficiently mature, a Node should implement a “best effort” by following the published intent of functionality and monitor or participate in the relevant specification development body. [BP1685]

Example

GIG Key Interface Profiles (KIPs) provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces.



☑ Refined Operational View

☑ Refined System View

☑ Interface Control Specifications -- Interface Control Document (ICD)

☑ Technical View & SV-TV Bridge

☑ Configuration Management Plan

☑ Procedures for standards conformance and interoperability testing utilizing reference implementations

☑ Engineering Management Plan

	Communications KIPs
1.	Logical Networks to DISN Transport Backbone
2.	Space to Terrestrial Interface
3.	JTF to Coalition
4.	JTF Component to JTF Headquarters
5.	Teleport (i.e., deployed interface to DISN)
6.	Joint Interconnection Service
7.	DISN Service Delivery Node
8.	Secure Enclave Service Delivery Node (e.g., SCI/Collateral KIP)
	Computing KIPs
9.	Application Server to Database Server
10.	Client to Server
11.	Applications to COE/CCP (NCES/GES)
	Network Operations KIPs
12.	End System to PKI
13.	Management Systems to (integrated) Management Systems
14.	Management Systems to Managed Systems
15.	IDM to Distribution Infrastructure
16.	Information Servers to IDM Infrastructure
	Applications
17.	Application Server to Shared Data - MOP (SADI)

Reference

- http://akss.dau.mil/dag/Guidebook/IG_c7.3.4.2.asp

2.4.1.9 Integrated Architectures

The DoD Architecture Framework (DoDAF) provides the rules, guidance, and product descriptions for developing and presenting architecture descriptions to ensure a common denominator for understanding, comparing, and integrating architectures. An integrated architecture consists of multiple views or perspectives (Operational View [OV], Systems View [SV], Technical Standards View [TV] and All-Views [AV]) that facilitate integration and promote interoperability across capabilities and among related integrated architectures.

- The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions.
- The SV is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions.
- The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.
- The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture.

The GIG architecture describes the basic, high level architecture in which Nodes reside. It is an integrated architecture consisting of the various DoDAF views. It provides a common lexicon and defines a basic infrastructure for the performance of information exchanges with other Global Information Grid (GIG) Nodes using the GIG Enterprise Services (GES) and the Net-Centric Enterprise Services (NCES). The GIG Architecture can be viewed https://disain.disa.mil/ncow/gigv2/index.htm; the home page for both the GIG architecture and

Net-Centric Operations and Warfare Reference Model (NCOW RM) is https://disain.disa.mil/ncow.html (user registration required).

Best Practice

- Nodes that will be part of the Global Information Grid (GIG) must be consistent with the GIG integrated architecture. [BP1635]

References

- DoD Architecture Framework (DoDAF), http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_I.pdf
- The GIG Architecture, https://disain.disa.mil/ncow/gigv2/index.htm
- The NCOW RM, https://disain.disa.mil/ncow.html

2.4.2 Core Enterprise Services (CES)

- Directory Services
- Security Services
- Services Management
- Service Discovery
- Content Discovery Services
- Mediation Services
- Collaboration Services
- Machine-to-Machine Messaging

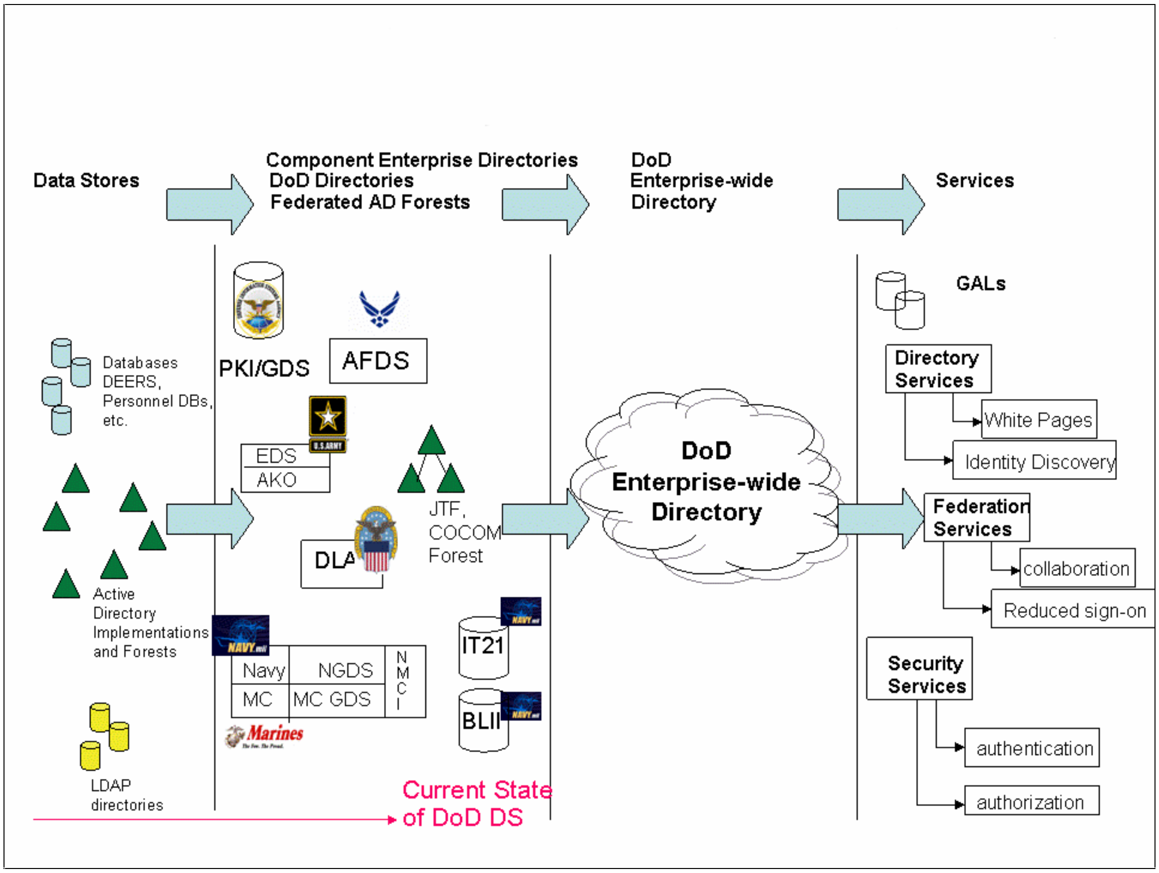
2.4.2.1 Directory Services

Secure inter-node interoperability relies heavily on the ability to lookup information about people and objects or devices across the breadth of the Global Information Grid (GIG). The technology that supports this is called directory services. In the Net-Centric Enterprise Services (NCES) service taxonomy, this falls under the scope of the CES Discovery Service for person and device discovery).

Nodes routinely use directory services today, such as Microsoft Active Directory and the DoD Public Key Infrastructure (PKI) Global Directory Service (GDS). Although implementations are widespread across the GIG, there is limited coordination and synchronization, creating pockets of information that must be unified. There are also substantial differences among implementations, including naming conventions. This situation is made more complex by the fact that these directories are typically also integral to a Node's security and system administration, supporting such basic functions as user login.

Coordination efforts at the level of the GIG within the DoD are underway to address these challenges. The DoD CIO directed DISA to develop a roadmap for directory services for the GIG. That roadmap is in draft form and is the product of the Joint Enterprise Directory Services Working Group (JEDIWG), which maintains a Web site at https://gesportal.dod.mil/sites/JEDIWG/default.aspx. This working group oversees both the Joint Directory Services Working Group (JDSWG) that focuses on PKI related requirements addressed by the Global Directory Service (GDS) as well as the DoD Active Directory

Interoperability Working Group (DADIWG). A snapshot of directory services evolution is in the diagram below:



Best Practices

- Nodes should provide a Commercial off-the-shelf Directory Service that can be used by all the Components. [BP1625]

- Node implemented directory services should comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1637]

- Node directory services proxies should be comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1638]

- Node interfaces to Components for directory services should align with the guidance being provided by the JEDIWG and sub-working groups, including such guidance as naming conventions, federation, and synchronization. [BP1686]

- Active Directory naming should follow the conventions defined in "Active Directory User Object Attributes Specification," as required by DoD CIO memorandum, "Microsoft Active Directory (AD) Services." [BP1687]

2.4.2.2 Security Services

Net-centric information exchanges will require security. The security mechanisms must be understood and implemented Global Information Grid (GIG)-wide because the information exchanges may occur between any Nodes on the GIG.

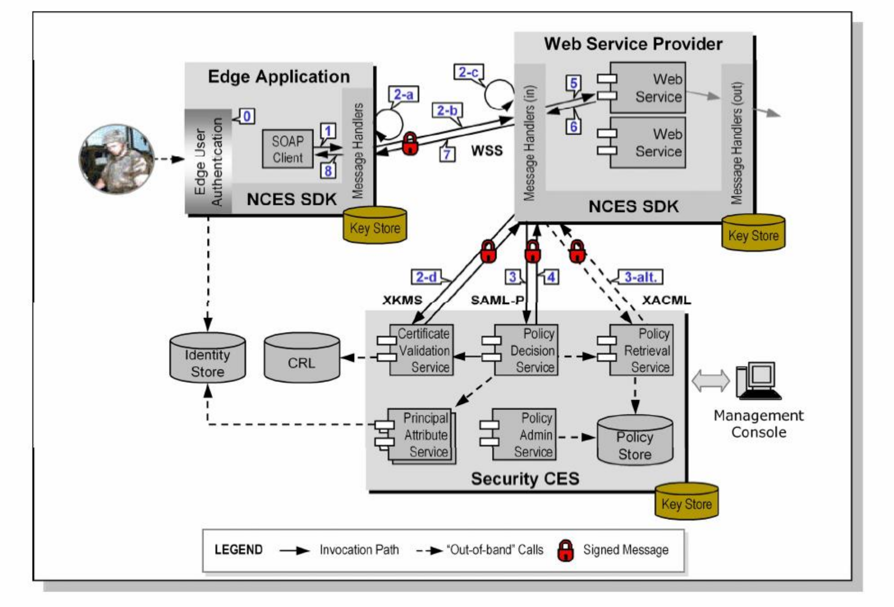
The CES approach to providing these GIG-wide security mechanisms is based on the DoD Public Key Infrastructure (PKI). Several security services in multiple categories of functionality are defined or planned, as shown in the following table. Generally, these services add to the DoD PKI authentication capabilities, providing a more complete set of security capabilities to applications, infrastructure, or other services.

Security Service Categories	Current Services	Future Services
Credential Mgmt Services	Certificate Validation Service	Certificate Retrieval Service Certificate Registration Service
Authorization Services	Policy Decision Service Policy Retrieval Service Policy Administration Service	Policy Subscription Service
Attribute Services	Principal Attribute Service	Resource Attribute Service Environment Attribute Service
Security Context Services	None	Security Context Service
Auditing & Logging Services	None	Security Logging Service Auditing Service

The figure below shows the relationship and typical interactions of these elements for a typical Web client invocation of a Web service. Software Development Kits (SDKs) are being developed to make these interactions easier to implement.

Node implementation of the elements shown below presents some critical design choices. The figure does not show, for instance, where each of the elements found in the "Security CES" box are hosted. There is active debate over this and related topics.

Authorization decisions should be the local purview of the Nodes, based on enterprise standards for identity, attributes, and policies, augmented and tailored locally to suit any unique requirements a Node may have. Furthermore, because security decisions can be computationally intensive and frequent, locally hosted implementations may be warranted by performance. Therefore, CES Security Services for authorization and policy decisions should be hosted locally on a Node. This requires coordination with DISA to implement these services on the local Node, and the overall approach may change as the Security Services are more fully developed and piloted.



Implementation topics for near term consideration are Identity Management, authentication, and authorization.

- Identity Management
- Public Key Infrastructure (authentication, and authorization)

2.4.2.2.1 Identity Management

Identity is an essential part of the CES Security Services, but Identity Management is not addressed in CES Increment 1. Identities of Global Information Grid (GIG) entities, human and non-human (i.e., services), must be unique across the GIG. DoD PKI X.509 certificates reserve a field to contain identity data, but there are issues today with how that field is populated for certain populations of users (e.g., coalition partners), and how to handle non-person entities. These issues are described in the paper entitled "Net-Centric Enterprise Services SOA Foundation Product Line, Service Security Component, Whitepaper: Service Identity Management and Credentialing."

While a universal solution for Identity Management is not yet defined, it is possible to make progress in the implementation of these services, particularly for Web applications and services with U.S. users having a CAC identification card holding DoD PKI X.509 certificates.

Identity is not as well understood and defined for non-person entities, such as services that may be part of a long invocation chain that is part of a workflow or orchestrated to yield a specific answer to a service invocation. Web server credentialing, though, has been defined to rely upon the DNS name of the site for identification.

The Net-Centric Enterprise Services (NCES) and Public Key Infrastructure (PKI) program offices are working on the challenges of non-person Identity Management, and an RFI has been issued to identify potential solutions.

Best Practice

- Use DoD PKI X.509 certificates for serves. [BP1652]

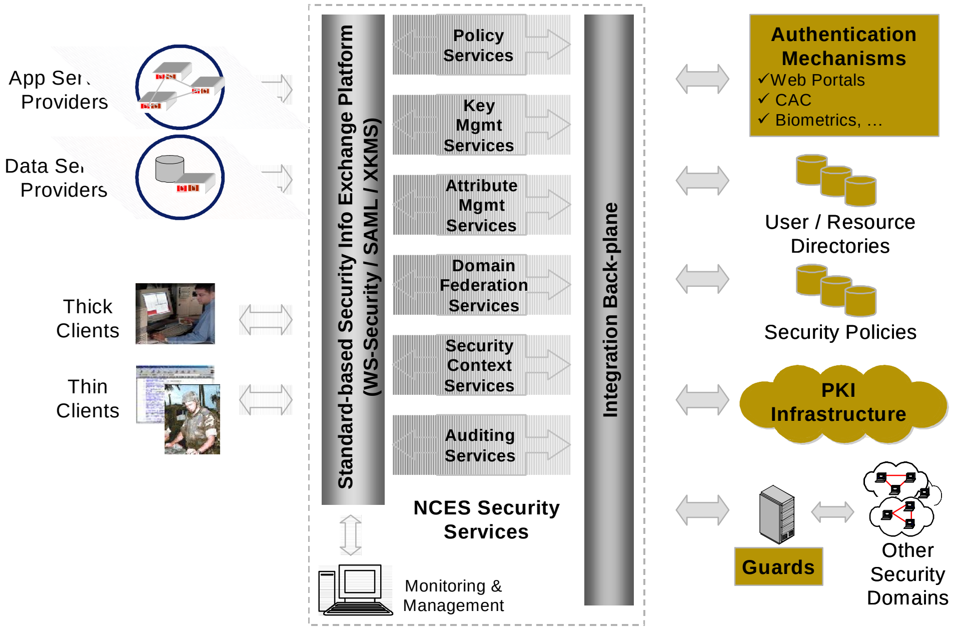
2.4.2.2.2 Public Key Infrastructure

Net-Centric Enterprise Services (NCES) Security Services rely heavily on Public Key Infrastructure (PKI) and Public Key (PK) Enabling (PKE). PKI provides an assured way for enabled applications to authenticate both intra-node and inter-node. PKI supports the concept of a single login across the enterprise, but legacy non-PK-enabled applications and services mean that username and password synchronization is also needed to support the single login concept; however, this is only practical in a limited sense (i.e., not the entire GIG). There remain some PKI implementation challenges, such as the implementation of the process for validating that an entity's certificate has not been revoked. Some COTS products, including some Web Application Containers, do not support the use of the Online Certificate Status Protocol (OCSP) or do not provide a capability to do file-based checking of the older Certificate Revocation List (CRL).

Nodes having both DoD and Intelligence Community (IC) systems and networks will also face the fact that the DoD and IC have implemented separate PKIs (including the dependent Directory Services). In general, the DoD PKI operates on the collateral classification networks, and the IC PKI operates on the SCI classified networks. Nodes may have to interface with multiple PKIs, therefore, depending on the systems and security levels at the Node. This presents some additional challenges when cross-domain interoperation is required, whether intra- or inter-node.

Nodes that have multinational or coalition personnel accessing the system will also encounter a challenge in obtaining CACs containing PKI certificates for these persons. The process is not well defined. As DoD moves further into the net-centric concepts, obtaining certificates for non-human entities in multinational or coalition systems will also be a challenge.

Authorization based on attributes corresponding to an entity is a practical way to implement authorization, provided that the enterprise can agree on the definitions of the attributes, policy, and a way of securely communicating and validating role membership. Unfortunately, attribute definitions and common security policy are not defined yet for the Global Information Grid (GIG), and Nodes are forced to use interim approaches, such as Windows AD or NIS group memberships, and evolve to a uniform definition of GIG roles and policies. Federation has not been addressed sufficiently to provide specific guidance.



2.4.2.3 Services Management

Net-centric operations can create mutual, mission-dependent obligations between Nodes. Service Management affects Node interoperability in that failure to provide services according to advertised capabilities or negotiated Service Level Agreements (SLAs) is essentially non-interoperability in the performance dimension.

Net-Centric Enterprise Services (NCES) services management capabilities are under development, but, as indicated in the current NCES schedule, are not scheduled for fielding until CES Increment 2.

Best Practice

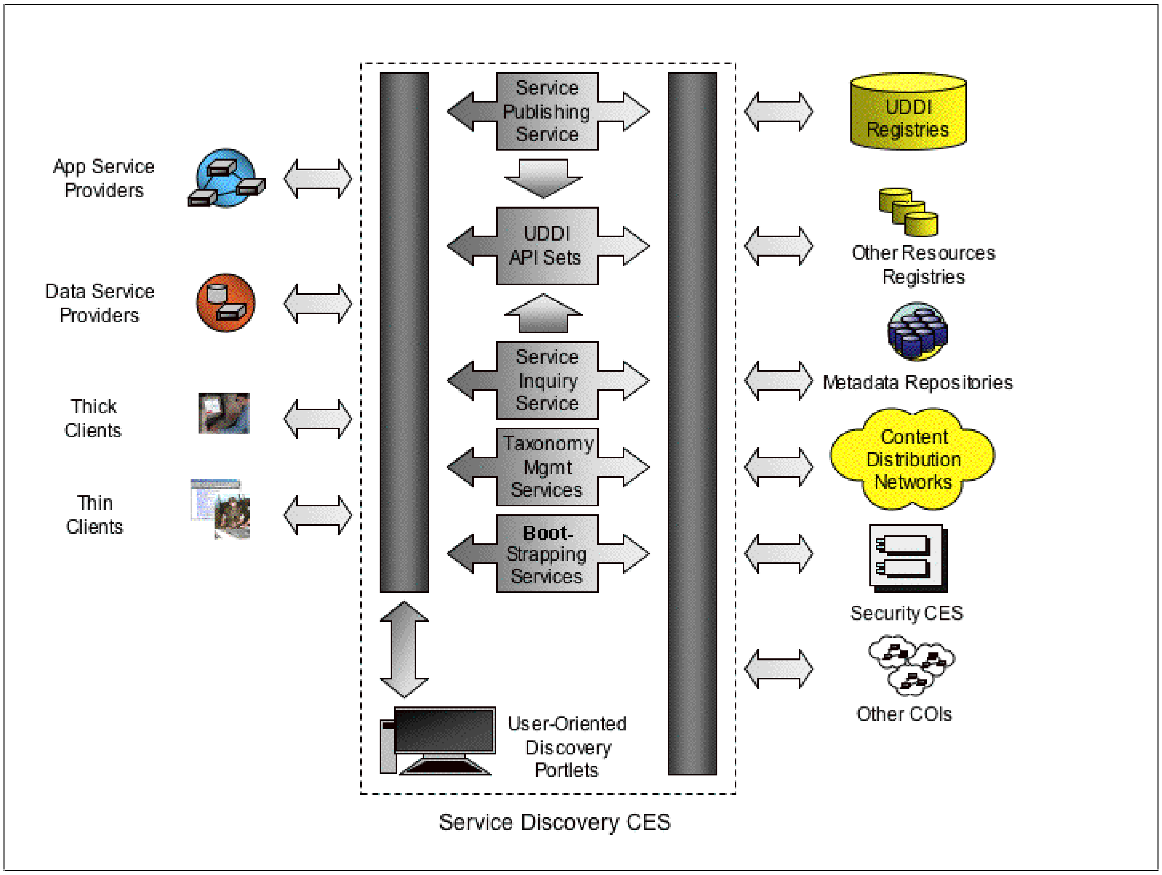
- For Services Management use an interim solution of instrumentation of services and external monitoring. [BP1688]

2.4.2.4 Service Discovery

Loosely coupled, net-centric information and services must be discoverable. That is, Nodes and Components must be able to discover dynamically where Component services and information reside in the Global Information Grid (GIG) and bind to those providers at runtime. The discovery concept relies upon the use of registries that are human and machine usable, for maintaining meta-data descriptions of information and services.

In Net-Centric Enterprise Services (NCES), service discovery is implemented by the CES Service Discovery (SD) services. Scheduled for CES Increment 1 fielding, a pilot implementation of SD services is available. The construction of registry entries is specified by the Service Definition Framework (SDF). The following figure shows the overall SD services architecture. Web portlets are being developed to assist in using the service, providing support for service publishing, searching, and browsing. The service registry implementation uses the Universal Description, Discovery, and Integration (UDDI) registry underneath, and the portlets use the UDDI application programming interface (API). An SD Portlet users guide describes how to use the portlets to access the registry.

Nodes again face several implementation choices regarding alignment of Components and Nodes approaches. Components exposed by the Node should be described as specified by the SDF and registered with the DISA hosted registries so that the Components services are visible to other Nodes. The pilot program should be used to practice and exercise the mechanics of service discovery and late binding. If the pilot implementation is not reachable, such as might be the case in a higher classified environment, the Node managers should coordinate amongst themselves and DISA to provide pilot and full service implementations that are reachable. Internal-facing services that are not likely to be of value beyond the Node's boundaries do not have to be discoverable, though it is a recommended best practice. If used internally, though, service discovery should be implemented for high availability.



Best Practices

- Components exposed by the Node should be described as specified by the Service Definition Framework (SDF). [BP1639]

- Components exposed by the Node should be registered with the DISA hosted registries. [BP1640]

- Node implemented Service Discovery (SD) should comply with the Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1641]

- Node Service Discovery (SD) proxies should be comply with the Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1642]

- The Service Discovery (SD) pilot program should be used to practice and exercise the mechanics of service discovery and late binding. [BP1689]

- Node implemented Service Discovery (SD) should be implemented for high availability. [BP1690]

- Node implemented Service Discovery (SD) should be implemented to meet compartmentalization needs. [BP1691]

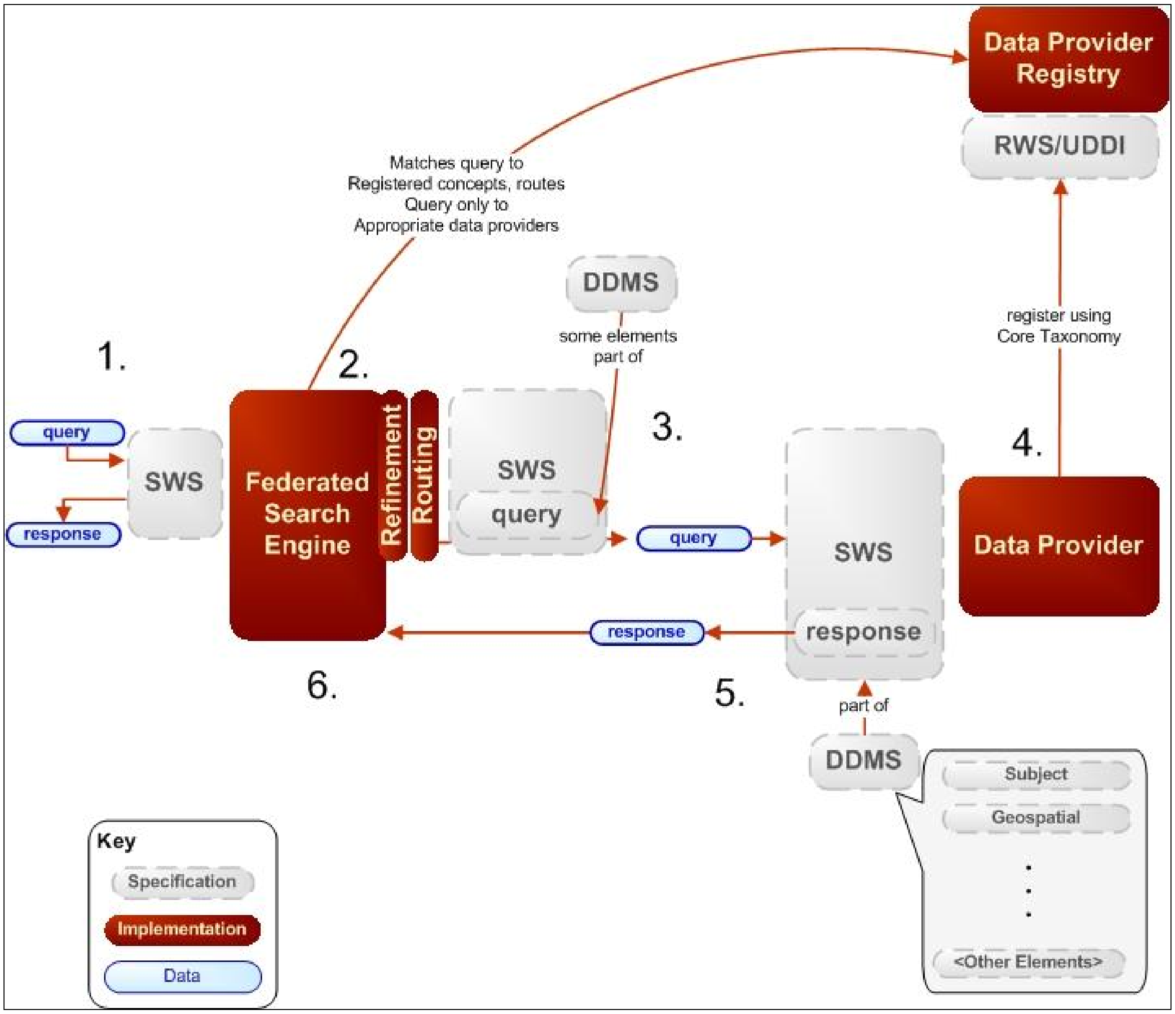
2.4.2.5 Content Discovery Services

Net-Centric Enterprise Services (NCES) includes a Content Discovery Service (CDS) that provides a Federated Search capability. That is, the service can search across a set of Content Discovery Services and yield an integrated result. The current approach to providing this service is to harness an existing capability termed "Federated Search" developed under the Horizontal Fusion (HF) program. The capability utilizes the DoD Discovery Metadata Specification (DDMS).

The Federated Search and DDMS document contains the following information:

> *Federated Search is implemented as a set of cooperating Web services. These services talk to each other using a common specification. The specification defines how a query and the results from that query are communicated. It describes not only the meaning, but also the format of the data that is exchanged between the services.*
>
> *The Defense Discovery Metadata Specification (DDMS) is used in the Federated Search specification to represent the concepts of a query as well as the resource result records, called meta cards, generated by a search result. Outgoing queries are matched against the resource meta cards by data providers to generate search results. It is the DDMS that ties the queries to the results and is used to express a common vocabulary.*

The following figure shows the Horizontal Fusion program's implementation of this Federated Search capability. Each Node should implement Federated Search - Registration Web Service (RWS) and Search Web Service (SWS). The RWS is used by data producers to register content sources and the SWS is used to search for content from the registered sources.



Best Practices

- Node implemented Federated Search - Registration Web Service (RWS) should comply with the Federated Search - Registration Web Service (RWS) Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1643]

- Node implemented Federated Search - Search Web Service (SWS) should comply with the Federated Search - Search Web Service (SWS) Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1644]

- The Node should implement local Content Discovery Service (CDS). [BP1645]

- Node Federated Search Services proxies should be comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs). [BP1646]

- The Node should provide access to the Federated Search Services. [BP1647]

- The Node should host the Registration Web Service (RWS) registration portlet. [BP1648]

2.4.2.6 Mediation Services

Published information may not always be in a format compatible with the subscriber's needs. The CES Mediation Service currently provides a capability to translate XML documents from one schema into another. To do this, the service uses Extensible Stylesheet Language Transformations (XSLT) and mappings DoD Metadata Registry. When XML document translation between schemas is a necessity, use the CES Mediation Service or a locally hosted copy thereof. Register developed mappings in the DoD Metadata Registry. (For additional information, see the Mediation Services perspective in *NESI Part 5: Developer Guidance*).

Best Practices

- Use the CES Mediation Service, or a locally hosted copy, when XML document translation between schemas is a necessity. [BP1711]

- Register developed mappings in the DoD Metadata Registry. [BP1712]

2.4.2.7 Collaboration Services

Collaboration tools provide a virtual meeting room environment for human interaction. The virtual environment enables multimedia collaboration (text, voice, and video) in multiple modes (person-to-person, open chat, restricted meeting, etc.) and application broadcasting and sharing.

A suite of collaboration tools and standards called the Defense Collaboration Tool Suite (DCTS) has been validated for interoperability by the DISA Joint Interoperability Test Command (JITC) and is used operationally. The DCTS Collaboration Management Office (CMO) within DISA is responsible for fielding, sustaining, and managing the life cycle of DCTS. Collaboration products approved for interoperability are listed at http://jitc.fhu.disa.mil/washops/jtcd/dcts/dctsv2 _software_list.html. Products certified for use on Secret Internet Protocol Router Network (SIPRNET) are listed at http://jitc.fhu.disa.mil/washops/jtcd/dcts/projects.html.

Net-Centric Enterprise Services (NCES) will provide a Collaboration Service. A pilot of a Next Generation Collaboration Service (NGCS) was recently concluded and has resulted in a Collaboration Service Request for Quotation (RFQ). The RFQ can be viewed at https://www.ditco.disa.mil/dcop/public/asp/requirement.asp?req_no=NCES_COLLABRFQ. This RFQ states an intention to select two competitive vendors for both the NIPRNET and SIPRNET communities, allowing users a choice of services. Provisions are also made within the RFQ for Offerors to propose solutions for providing service in degraded environments, such as low bandwidth, and in other networks and separated enclaves. It is possible for services to be operational during 2006. The schedule indicates that progress on fielding the Collaboration Service should be monitored closely in the near term, and take steps to determine actively which vendor offering to employ (perhaps hosting at the Node) if in a disadvantaged environment or separate network.

The recent DOD CIO memorandum, “DoD Collaboration Policy Update,” requires use of the NCES Collaboration Services that are under development. It also provides policy for urgent requirements until the NCES services are operational. Collaboration products used to satisfy urgent requirements should be approved and from the list on the aforementioned Web sites, until the NCES Collaboration Service is available.

Best Practices

- The schedule indicates that progress on fielding the Collaboration Service should be monitored closely in the near term; take steps to determine actively which vendor offering to employ (perhaps hosting at the Node) if in a disadvantaged environment or separate network. [BP1692]

- Collaboration products used to satisfy urgent requirements should be approved and from the JTIC list (see http://jitc.fhu.disa.mil/washops/jtcd/dcts/dctsv2 _software_list.html and, for products certified for use on SIPRNET, http://jitc.fhu.disa.mil/washops/jtcd/dcts/projects.html) until the Net-Centric Enterprise Services (NCES) Collaboration Service is available. [BP1693]

2.4.3 Machine-to-Machine Messaging

Net-Centric Enterprise Services (NCES) is defining services for machine-to-machine messaging, similar in capability to services offered by several COTS vendors of Enterprise Service Busses (ESBs). ESBs, though, are not yet interoperable enough to support messaging between arbitrary Global Information Grid (GIG) Nodes using different ESBs. NESI guidance is TBD until this service is better defined.

Glossary

Term	Acronym	Definition
Access Control List	**ACL**	In computer security, ACL is a concept used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identity. In networking, ACL refers to a list of ports and services that are available on a host, each with a list of hosts and/or networks permitted to use the service. Both individual servers as well as routers can have access lists. Access lists are used to control both inbound and outbound traffic, and in this context they are similar to firewalls. http://en.wikipedia.org/wiki/Access_control_list
Active Directory	**AD**	An implementation of Lightweight Directory Access Protocol (LDAP) directory services by Microsoft for use in Windows environments; allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization. An Active Directory stores information and settings relating to an organization in a central, organized, accessible database. Active Directory networks can vary from a small installation with a few hundred objects, to a large installation with millions of objects. http://en.wikipedia.org/wiki/Active_Directory
All-Views	**AV**	The DoDAF All-Views (AV) products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and timeframe for the architecture. The setting in which the architecture exists comprises the interrelated conditions that compose the context for the architecture. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions. DoDAF v1 Vol. 1, 9 Feb 2004, page 1-3, section 1.3.4

Term	Acronym	Definition
Application		Provides the resources necessary to provision, operate and maintain Net-Centric Enterprise Services (NCES) capabilities.
Assistant Secretary of Defense for Networks and Information Integration	**ASD/NII**	The Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) is also the DoD Chief Information Officer (CIO).
Browser		Short for *Web browser*, a software application used to locate and display Web pages. http://www.webopedia.com/TERM/b/browser.html
Capability Development Document	**CDD**	A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability. CJCSI 3170.01E, 11 May 2005, Glossary page GL-5
Capability Production Document	**CPD**	A document that addresses the production elements specific to a single increment of an acquisition program. CJCSI 3170.01E, 11 May 2005, Glossary page GL-5
Certificate		In computing and especially computer security and cryptography, the word *certificate* generally refers to a digital identity certificate, also known as a Public Key (PK) certificate. It also may be awarded as a necessary certification to validate that a student is considered competent in a certain specific networking skill area in today's ubiquitous and necessary Information Technology (IT). http://en.wikipedia.org/wiki/Certificate
Certificate Revocation List	**CRL**	A list of certificates (more accurately: their serial numbers) which have been revoked, are no longer valid, and should not be relied upon by any system user. http://en.wikipedia.org/wiki/Certificate_revocation_list

Term	Acronym	Definition
Chief Information Officer	**CIO**	Job title for a manager responsible for Information Technology (IT) within an organization; often reports to the chief executive officer or chief financial officer. For information on the ASD/ Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) DoD CIO see DoDD 5144.1 of 2 May 2005. http://en.wikipedia.org/wiki/Chief_Information_Officer
Cipher Text	**CT**	Data that has been encrypted. Cipher text is unreadable until it has been converted into Plain Text (PT) (decrypted) with a key. http://www.webopedia.com/TERM/C/cipher_text.html
Collaboration		Allows users to work together securely on the network by way of video, audio, text chat, white boarding, online meetings, work groups, application sharing.
Collaboration Management Office	**CMO**	DISA organization responsible for fielding, sustaining and managing the life cycle of the Defense Collaboration Tool Suite (DCTS)
Commercial Off-The-Shelf	**COTS**	Products which are ready-made and available for sale to the general public. http://en.wikipedia.org/wiki/COTS
Common Access Card	**CAC**	A DoD-wide smart card used as the identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals; the primary platform for the Public Key Infrastructure (PKI) authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces as described in DoD Directive 8190.3, "Smart Card Technology," 31 August 2002. DoDI 88520.2.3, 1 April 2004, Enclosure (2) Definitions, page 13

Term	Acronym	Definition
Common Object Request Broker Architecture	**CORBA**	CORBA "wraps" code written in another language into a bundle containing additional information on the capabilities of the code inside, and explaining how to call it. The resulting wrapped objects can then be called from other programs (or CORBA objects) over the network. The CORBA specification defines APIs, communication protocol, and object/service information models to enable heterogeneous applications written in various languages running on various platforms to interoperate. http://en.wikipedia.org/wiki/CORBA
Community of Interest	**COI**	A collection of people who exchange information using a common vocabulary in support of shared missions, business processes, and objectives. The community is made up of the users/operators who participate in the information exchange, the system builders who develop computer systems for these users, and the functional proponents who define requirements and acquire systems on behalf of the users.
Component		In the context of a NESI Node, a Component can be a system, an application, a service, or another Node.
Computer Network Defense	**CND**	Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. http://www.dtic.mil/doctrine/jel/doddict/data/c/01182.html
Computer Network Defense Service Provider	**CNDSP**	Those organizations responsible for delivering protection, detection and response services to its users. CNDS providers must provide for the coordination service support of a CNDS/CA. CNDS is commonly provided by a Computer Emergency or Incident Response Team (CERT/CIRT) and may be associated with a Network Operations (NetOps) and Security Center (NOSC). DoD Directive O-8530.1, Computer Network Defense (CND), 8 January 2001, Enclosure 2 Definitions, page 12
Content Discovery Service	**CDS**	Net-Centric Enterprise Services (NCES) service that provided a Federated Search capability.

Term	Acronym	Definition
Core Enterprise Services	**CES**	Generic information services that apply to any COI, provide the basic ability to search the enterprise for desired information, and then establish a connection to the desired service. http://www.defenselink.mil/nii/org/cio/doc/GIG_ES_Core_Enterprise_Services_Strategy_V1-1a.pdf
Defense Acquisition University	**DAU**	Combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. http://www.disa.mil/main/about/missman.html
Defense Collaboration Tool Suite	**DCTS**	A flexible, integrated set of applications providing interoperable, synchronous and asynchronous collaboration capability to the DoD agencies, Combatant Commands and Military Services. http://www.disa.mil/main/prodsol/dcts.html
Defense Enterprise Computing Center	**DECC**	DISA's five Defense Enterprise Computing Centers (DECCs) and their detachments operate hardware and software encompassing a broad spectrum of computing, storage and communications technologies. http://www.disa.mil/main/about/csc.html
Defense Information Systems Agency	**DISA**	Combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. http://www.disa.mil/main/about/missman.html
Design Pattern		General repeatable solution to a commonly-occurring problem in software design. A design pattern isn't a finished design that can be transformed directly into code; it is a description or template for how to solve a problem that can be used in many different situations. http://en.wikipedia.org/wiki/Design_pattern_%28computer_science%29
Discovery		Search, locate or publish data (content), other capabilities (services), or users across the Global Information Grid (GIG).

Term	Acronym	Definition
Document Object Model	**DOM**	A description of how an HTML or XML document is represented in an object-oriented fashion; DOM provides an application programming interface to access and modify the content, structure and style of the document. http://en.wikipedia.org/wiki/Document_Object_Model
DoD Active Directory Interoperability Working Group	**DADIWG**	
DoD Architecture Framework	**DoDAF**	Defines a common approach for DoD architecture description, development, presentation, and integration for both warfighting operations and business processes [DoDAF v1.0 supersedes C4ISR Architecture Framework v2.0, 18 December 1997]. Office of the Secretary of Defense memo of 9 Feb 2004, "The Department of Defense Architecture Framework (DoDAF)"
DoD Discovery Metadata Specification	**DDMS**	Defines discovery metadata elements for resources posted to community and organizational shared spaces. DDMS v1.3, 29 July 2005
DoD Web Services Profile		Provides specifications and implementation guidelines to maximize interoperability across DoD Web Service implementations.
Domain Name System [or Service or Server]	**DNS**	An Internet service that translates domain names into Internet Protocol (IP) addresses. http://www.webopedia.com/TERM/D/DNS.html
Dynamic Host Configuration Protocol	**DHCP**	A protocol for assigning dynamic Internet Protocol (IP) addresses to devices on a network; DHCP a device can have a different IP address every time it connects to the network. http://www.webopedia.com/TERM/D/DHCP.html

Term	Acronym	Definition
Electronic Data Interchange Personnel Identifier	**EDI-PI**	A unique number assigned to each recipient of a Common Access Card (CAC), which is issued by the United States Department of Defense through the Defense Enrollment Eligibility Reporting System (DEERS). http://en.wikipedia.org/wiki/Electronic_Data_Interchange_Personal_Identifier
Electron-Trapping Optical Memory	**eTOM**	A method of erasable optical storage. Information is written, or stored, by a low-power laser tuned to a specific frequency. The laser elevates the energy level of electrons to a trapped state. The data is read by a second laser that returns the elevated electrons to their ground state. http://www.webopedia.com/TERM/E/ETOM.html
End-to-End	**E2E**	The end-to-end principle is one of the central design principles of the Internet Protocol (IP) that is the basis of the Internet. It states that, whenever possible, communications protocol operations should be defined to occur at the end-points of a communications system. In any computer communication, there are n >= 2 end points, called "end systems" or "hosts". End-to-end security means that sensitive data is encrypted all the way from your device side application back to the enterprise. Rather than relying on transport-level security such as Secure Socket Layer (SSL), end-to-end security puts the power of strong encryption in your hands, all through a simple interface. This ends the so-called “air gap” where sensitive data was previously decrypted at the gateway during translation for wireless protocols into Internet protocols. End-to-end monitoring is the process of attempting to access a Web server or other Internet device from across the Internet, just as a real end user would, to verify that the server is accessible and functioning properly at all times. This approach can be used instead of, or as a complement to, local monitoring software run by the Web Administrator. http://en.wikipedia.org/wiki/End-to-end

Term	Acronym	Definition
Enterprise		An organization considered as an entity or system that includes interdependent resources (e.g., people, organizations, and technology) that must coordinate functions and share information in support of a common mission or a set of related missions. In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet, for example, is a good example of an enterprise computing system. http://www.webopedia.com/TERM/e/enterprise.html
Enterprise Management Services	**EMS**	Enterprise Management Services (EMS) which are often used internal to a node, using a variety of COTS tools, which are fundamental to execution of Service Level Agreements (SLAs).
Enterprise Service Management		Monitor/manage Global Information Grid (GIG) Enterprise Services against operational performance parameters to ensure reliability and availability of critical capabilities.
Enterprise Services		In the DoD Global Information Grid (GIG) context, a set of services which provide visibility, access and delivery of data, and information services across the DoD enterprise.
eXtensible Access Control Markup Language	**XACML**	A declarative access control policy language implemented in XML. http://en.wikipedia.org/wiki/XACML

Term	Acronym	Definition
Extensible Markup Language	**XML**	A World Wide Web Consortium (W3C)-recommended general-purpose markup language for creating special-purpose markup languages, capable of describing many different kinds of data. In other words: XML is a way of describing data and an XML file can contain the data too, as in a database. It is a simplified subset of Standard Generalized Markup Language (SGML). The primary purpose is to facilitate the sharing of data across different systems, particularly systems connected via the Internet. Languages based on XML (for example, Geography Markup Language (GML), RDF/XML, RSS, MathML, Physical Markup Language (PML), XHTML, SVG, MusicXML and cXML) are defined in a formal way, allowing programs to modify and validate documents in these languages without prior knowledge of their form. http://en.wikipedia.org/wiki/Xml
Extensible Stylesheet Language Transformations	**XSLT**	An XML-based language used for the transformation of XML documents. The original document is not changed; rather, a new document is created based on the content of an existing document. The new document may be serialized (output) by the processor in standard XML syntax or in another format, such as HTML or Plain Text (PT). XSLT is most often used to convert data between different XML schemas or to convert XML data into Web pages or PDF documents. http://en.wikipedia.org/wiki/Xslt
Façade Design Pattern		An object that provides a simplified interface to a larger body of code, such as a class library. http://en.wikipedia.org/wiki/Facade_pattern
Federated Search		Implementation of a computer program that allows users to access multiple data sources with a single query string located within a single interface. http://en.wikipedia.org/wiki/Federated_search
Firewall		A piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.

Term	Acronym	Definition
GIG Router Working Group	**GRWG**	
Global Information Grid	**GIG**	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. DoDD 8100.1, 19 September 2002, "Global Information Grid (GIG) Overarching Policy"
Global Positioning System	**GPS**	A satellite constellation that provides highly accurate position, velocity, and time navigation information to users. [JP 1-02] http://www.dtic.mil/doctrine/jel/doddict/data/g/02300.html
High Assurance Internet Protocol Encryption	**HAIPE**	DoD version of Internet Protocol (IP) security (IPsec) protocol. http://en.wikipedia.org/wiki/HAIPE
Horizontal Fusion	**HF**	Horizontal Fusion (HF) is a direct response to Secretary of Defense Donald H. Rumsfeld's vision of Force Transformation. It demonstrates the ability to use lightweight automation to replace system mass with superior access to information based on a coherent architecture for an arbitrary future. Horizontal Fusion acts as a catalyst by implementing and demonstrating technologies and techniques that significantly advance the process of information-sharing in a an evolving net-centric environment. http://horizontalfusion.dtic.mil/vision/
IA/Security		Authorizes and authenticates Global Information Grid (GIG) users to ensure the confidentiality and integrity of information and services.
Identity Management		Provides the methodology and functions for maintaining information on people, consumers, and service providers. Supports the validation of identity authentication credentials.

Term	Acronym	Definition
Information Assurance	**IA**	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. CNSS Instruction No. 4009, Revised May 2003, "National Information Assurance (IA) Glossary"
Information Assurance Support Environment	**IASE**	DoD IA Portal managed by DISA. http://iase.disa.mil/index2.html
Information Support Plan	**ISP**	Used by program authorities to document the IT and National Security Systems (NSS) needs, objectives, interface requirements for all non-ACAT and fielded programs. CJCSI 6212.01C, 20 Nov 2003, Glossary page GL-11
Information Technology	**IT**	Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. The term "IT" includes National Security Systems (NSS). CJCSI 6212.01C, 20 Nov 2003, Glossary page GL-8
Information Technology Laboratory	**ITL**	The ITL at the National Institute of Standards and Technology (NIST) has the broad mission of supporting U.S. industry, government, and academia with measurements and standards that enable new computational methods for scientific inquiry, assure IT innovations for maintaining global leadership, and re-engineer complex societal systems and processes through insertion of advanced Information Technology (IT). http://www.itl.nist.gov/itl-what_itl_does.html
Intelligence Community	**IC**	A federation of executive branch agencies and organizations that conduct intelligence activities necessary for conduct of foreign relations and protection of national security. http://www.intelligence.gov/

Term	Acronym	Definition
Internet Protocol	**IP**	Data packets routed across network, not switched via dedicated circuits.
Internet Protocol Version 4	**IPv4**	Version 4 of the Internet Protocol (IP). It was the first version of the Internet Protocol to be widely deployed, and forms the basis for most of the current Internet (as of 2004). It is described in IETF RFC 791, which was first published in September, 1981. IPv4 uses 32-bit addresses, limiting it to 4,294,967,296 unique addresses, many of which are reserved for special purposes such as local networks or multicast addresses. This reduces the number of addresses that can be allocated as public Internet addresses. As the number of addresses available is consumed, an IPv4 address shortage appears to be inevitable in the long run. This limitation has helped stimulate the push towards Internet Protocol Version 6 (IPv6), which is currently in the early stages of deployment, and may eventually replace IPv4. http://en.wikipedia.org/wiki/IPv4
Internet Protocol Version 6	**IPv6**	Version 6 of the Internet Protocol (IP); it was initially called IP Next Generation (IPng) when it was picked as the winner in the IETF's IPng selection process. IPv6 is intended to replace the previous standard, Internet Protocol Version 4 (IPv4), which only supports up to about 4 billion (4 × 10^9) addresses. IPv6 supports up to about 3.4 × 10^{38} (340 undecillion) addresses. This is the equivalent of 4.3 × 10^{20} (430 quintillion) addresses per square inch (6.7 × 10^{17} (670 quadrillion) addresses/mm²) of the Earth's surface. It is expected that IPv4 will be supported until at least 2025, to allow time for bugs and system errors to be corrected. http://en.wikipedia.org/wiki/Ipv6
Intrusion Detection System	**IDS**	Inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. http://www.webopedia.com/TERM/i/intrusion_detection_system.html
Java 2 Platform, Enterprise Edition	**J2EE**	See the Java Platform, Enterprise Edition (Java EE) entry http://java.sun.com/javaee/index.jsp

Term	Acronym	Definition
Java Platform, Enterprise Edition	**Java EE**	Industry standard for developing portable, robust, scalable and secure server-side Java applications. Building on the solid foundation of Java SE, Java EE provides Web services, component model, management, and communications APIs that make it the industry standard for implementing enterprise class service-oriented architecture (SOA) and Web 2.0 applications. The name of the Java platform for the enterprise has been simplified. Formerly, the platform was known as Java 2 Platform, Enterprise Edition (J2EE), and specific versions had "dot numbers" such as J2EE 1.4. The "2" is dropped from the name, as well as the dot number. So the next version of the Java platform for the enterprise is Java Platform, Enterprise Edition 5 (Java EE 5). http://java.sun.com/javaee/index.jsp
Joint Capabilities Integration and Development System	**JCIDS**	Establishes procedures to support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying, assessing and prioritizing joint military capability. CJCSI 3170.01E, 11 May 2005, “Joint Capabilities Integration and Development System”
Joint Directory Services Working Group	**JDSWG**	
Joint Enterprise Directory Services Working Group	**JEDIWG**	
Joint Interoperability Test Command	**JITC**	Independent operational test and evaluation/assessor of DISA and other DoD Command, Control, Communications, Computers and Intelligence (C4I) acquisitions. http://jitc.fhu.disa.mil/mission.htm

Term	Acronym	Definition
Joint Worldwide Intelligence Communications System	**JWICS**	The sensitive, compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. http://www.dtic.mil/doctrine/jel/doddict/data/j/02941.html
Key Interface Profile	**KIP**	An operational functionality, systems functionality and technical specifications description of the Key Interface. The profile consists of refined Operational and Systems Views, Interface Control Document/Specifications, Engineering Management Plan, Configuration Management Plan, Technical Standards View with SV-TV Bridge, and Procedures for Standards Conformance and Interoperability Testing. CJCSI 6212.01C, 20 November 2003, Glossary page GL-14
Legacy System		An existing computer system or application program which continues to be used because the user (typically an organization) does not want to replace or redesign it. http://en.wikipedia.org/wiki/Legacy_system
Lightweight Directory Access Protocol	**LDAP**	A networking protocol for querying and modifying directory services running over Transmission Control Protocol/Internet Protocol (TCP/IP); an LDAP directory usually follows the X.500 model. http://en.wikipedia.org/wiki/Ldap
Link-16		Tactical Data Information Link (TADIL) primarily designed for use by Command and Control (C2) and Air-to-Air assets; uses the Joint Tactical Data Link (TADIL-J) message format. http://aatc.aztucs.ang.af.mil/aatcinfo.htm
Machine-to-Machine Messaging		Provides reliable machine-to-machine message exchange across the enterprise.
Mediation		Translates, brokers, aggregates, fuses or integrates data into commonly understood formats.
Messaging		Distributed, machine-to-machine messaging for notifications and alerts.

Term	Acronym	Definition
Metadata Services		Provides access to Extensible Markup Language (XML) components, data elements, taxonomy galleries, and validation and generation tools for DOD software developers.
Multicast		The delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once and only create copies when the links to the destinations split. http://en.wikipedia.org/wiki/Multicast
MX Record		A Mail eXchange (MX) Record is a type of resource record in the Domain Name System (DNS) specifying how Internet e-mail should be routed; MX records point to the servers to send an e-mail to, and which ones it should be sent to first, by priority. http://en.wikipedia.org/wiki/MX_Record
National Institute of Standards and Technology	**NIST**	Non-regulatory federal agency within the U.S. Commerce Department's Technology Administration with a mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. http://www.nist.gov/public_affairs/general2.htm
National Security Agency	**NSA**	America’s cryptologic organization; it coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information. http://www.nsa.gov/about/index.cfm
National Security Systems	**NSS**	Any telecommunications or information system operated by the Department of Defense (DoD), the function, operation, or use of which involves 1) intelligence activities, 2) cryptologic activities related to national security, 3) the command and control of military forces, 4) equipment that is an integral part of a weapons system, or 5) criticality to the direct fulfillment of military or intelligence missions. Defense Acquisition Acronyms and Terms, Twelfth Edition, July 2005, page B108

Term	Acronym	Definition
Net-Centric Enterprise Services	**NCES**	The Net-Centric Enterprise Services (NCES) program provides enterprise-level Information Technology (IT) services and infrastructure components, also called Core Enterprise Services (CES), for the Department of Defense (DoD) Global Information Grid (GIG).
Net-Centric Implementation Directives	**NCIDs**	
Net-Centric Operations and Warfare Reference Model	**NCOW RM**	Describes the activities required to establish, use, operate, and manage the DoD net-centric enterprise information environment to include the generic user interface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest services, and environment control services), and the enterprise management components. CJCSI 6212.01C, 20 November 2003, Glossary page GL-16
Net-Ready Key Performance Parameter	**NR-KPP**	Measures the net-centricity of a new program or major upgrade.
Network Intrusion Detection	**NID**	Attempt to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic. http://en.wikipedia.org/wiki/Network_intrusion-detection_system

Term	Acronym	Definition
Network Operations	**NetOps**	An organizational, procedural, and technological construct for ensuring information and decision superiority at the strategic, operational, and tactical levels of warfare as well as within DOD business operations. NetOps is an operational approach, which addresses the interdependency and integration of IA/CND, S&NM, and CS capabilities. NetOps consists of the organizations, tactics, techniques, procedures, functionalities, and technologies required to plan, administer, and monitor use of the Global Information Grid (GIG) infrastructure and the end-to-end information flows of the GIG; and to respond to threats, outages, and other operational impact. NetOps ensures mission requirements are properly considered in GIG operational decision-making. NetOps enables the GIG to provide its users with information they need, when they need it, where they need it, with appropriate protection of the information. NetOps is an essential capability for successful execution of net-centric warfare and other net-centric operations in support of national security objectives. http://en.wikipedia.org/wiki/Netops
Network Time Protocol	**NTP**	Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. It is designed particularly to resist the effects of variable latency. http://en.wikipedia.org/wiki/Network_Time_Protocol
Networks and Information Integration	**NII**	See Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) entry; acronym also expands to National Information Infrastructure
New Generation Operations Support Systems	**NGOSS**	TeleManagement Forum (TMF) term for its description of the optimum way for a Communications Service Provider (CSP) to manage its business. It describes how to integrate Operational Support Systems (OSS) and provides technical deliverables to assist with this integration. http://en.wikipedia.org/wiki/NGOSS
Next Generation Collaboration Service	**NGCS**	DISA pilot for Services, Combatant Commands (COCOMs), and Defense agencies which concluded on 2 September 2005. http://www.disa.mil/ges.ngcs.html

Term	Acronym	Definition
Node		In general network usage, a node is a processing location such as a computer or some other device. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address. http://www.webopedia.com/TERM/n/node.html A NESI Node is a collection of integrated components (i.e., systems, applications, services and other Nodes) that are bound together spatially and/or temporally to meet the needs of a particular mission. It is conceptual in nature and can not be defined in terms of a concrete set of components or size. The membership of a component within a particular Node is not exclusive and a Component can be part of multiple Nodes.
Non-secure Internet Protocol Router Network	**NIPRNET**	Provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. Direct connection data rates range from 56Kbps to 155Mbps. Remote dial-up services are available up to 56Kbps. http://www.disa.mil/main/prodsol/data.html
Online Certificate Status Protocol	**OCSP**	Internet Protocol (IP) used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a Public Key Infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed *OCSP responders*. http://en.wikipedia.org/wiki/Ocsp
Operational View	**OV**	DoDAF description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions. DoDAF Volume I, 9 February 2004, Section 1.3.1, page 1-2

Term	Acronym	Definition
Orchestration		Co-ordination of events in a process; orchestration directs and manages the on-demand assembly of multiple component services to create a composite application or business process. http://looselycoupled.com/glossary/orchestration
Organization for the Advancement of Structured Information Standards	**OASIS**	A not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. *http://www.oasis-open.org/who/*
Plain Text	**PT**	Refers to textual data in ASCII format. Plain text is the most portable format because it is supported by nearly every application on every machine. It is quite limited, however, because it cannot contain any formatting commands. In cryptography, plain text refers to any message that is not encrypted. http://www.webopedia.com/TERM/p/plain_text.html
Platform		In computing, a platform describes some sort of framework, either in hardware or software, which allows software to run. Typical platforms include a computer's architecture, operating system, or programming languages and their runtime libraries. http://en.wikipedia.org/wiki/Platform_%28computing%29
Plug-in		A hardware or software module that adds a specific feature or service to a larger system. http://www.webopedia.com/TERM/p/plug_in.html
Portlet		A reusable Web component that displays relevant information to portal users. Examples for portlets include email, weather, discussion forums, and news. The purpose of the Web Services for Remote Portlets (WSRP) interface is to provide a Web services standard that allows for the "plug-n-play" of portals, other intermediary Web applications that aggregate content, and applications from disparate sources. The portlet specification enables interoperability between portlets and portals. This specification defines a set of APIs for portal computing that addresses the areas of aggregation, personalization, presentation, and security. http://en.wikipedia.org/wiki/Portlets

Term	Acronym	Definition
Protocol		An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, data compression method, if any, how the sending device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message http://www.webopedia.com/TERM/p/protocol.html
Proxy		A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers have two main purposes: improve performance and filter requests. http://www.webopedia.com/TERM/p/proxy_server.html
Public Key		One of a pair of cryptographic keys (public key and private key) to allow users to communicate securely without having prior access to a single shared cryptographic key. http://en.wikipedia.org/wiki/Public_key
Public Key Infrastructure	**PKI**	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. CNSS Instruction No. 4009, Revised May 2003, “National Information Assurance (IA) Glossary”
Quality of Service	**QoS**	Networking term that specifies a guaranteed throughput level. http://www.webopedia.com/TERM/Q/QoS.html
Registration Web Service	**RWS**	Horizontal Fusion (HF) service used by data producers to register content sources.
Request for Quotation	**RFQ**	A solicitation used in negotiated acquisition to communicate government requirements to prospective contractors and to solicit a quotation. A response to an RFQ is not an offer; however, it is informational in character. Defense Acquisition Acronyms and Terms, Twelfth Edition, July 2005, page B-140

Term	Acronym	Definition
Router		A device that forwards data packets along networks. A router is connected to at least two networks, commonly two local area networks (LANs) or wide area networks (WANs) or a LAN and its Internet Service Provider's network. Routers are located at gateways, the places where two or more networks connect. http://www.webopedia.com/TERM/r/router.html
Schema		The structure of a database system, described in a formal language supported by the database management system (DBMS). http://www.webopedia.com/TERM/s/schema.html
Search Web Service	**SWS**	Horizontal Fusion (HF) service used to search for content from registered sources.
SECRET Internet Protocol Router Network	**SIPRNET**	DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. Direct connection data rates range from 56 kbps to 155 Mbps for the Non-secure Internet Protocol Router Network (NIPRNET), and up to 45 Mbps for the SIPRNET. Remote dial-up services are also available, ranging from 19.2 kbps on SIPRNET to 56 kbps on NIPRNET. http://www.disa.mil/main/prodsol/data.html
Secure Socket[s] Layer	**SSL**	A technology that allows Web browsers and Web servers to communicate over a secured connection. The protocol runs above Transmission Control Protocol/Internet Protocol (TCP/IP) and below application protocols. http://java.sun.com/j2ee/1.4/docs/glossary.html
Security Assertion Markup Language	**SAML**	An XML standard for exchanging authentication and authorization data between security domains; that is, between an identity provider and a service provider. SAML is a product of the Organization for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee. Source: http://en.wikipedia.org/wiki/SAML

Term	Acronym	Definition
Security Technical Implementation Guide	**STIG**	Configuration standards for DOD IA and IA-enabled devices/systems. http://iase.disa.mil/stigs/index.html
Sensitive Compartmented Information	**SCI**	Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI). DoDD 8520.1, 20 December 2001, Subject: Protection of Sensitive Compartmented Information (SCI), Page 2, Section 3.3
Server		A computer or device on a network that manages network resources. http://www.webopedia.com/TERM/s/server.html
Service		A service is any function that has a clearly defined interface accessed through well-defined public access points.
Service Definition Framework	**SDF**	SDF provides service users, customers, developers, providers, and managers with a common frame of reference. Its structure and methodology enable you to fully define the Service Access Points (SAPs) for the service.
Service Discovery	**SD**	Provides a "yellow pages," categorized by DOD function, enabling users to advertise and locate capabilities available on the network.
Service Level Agreement	**SLA**	A contract between an Application Service Provider (ASP) and the end user which stipulates and commits the ASP to a required level of service. An SLA should contain a specified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee. http://www.webopedia.com/TERM/S/Service_Level_Agreement.html
Service Management		Enables monitoring of DOD Web services. Provides reporting of service-level information to potential and current service consumers, program analysts, and program managers.

Term	Acronym	Definition
Service Mediation		Allows disparate applications to work together across the enterprise by supporting the transformation of information from one format to another, and the correlation and fusion of data from diverse sources. Supports creation and implementation of process workflows across the enterprise.
Service Security		Provides a layer of Defense in Depth that enables protection, defense, and integrity of the information environment.
Simple Object Access Protocol	**SOAP**	A lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet Protocols (IPs), including SMTP, MIME, and HTTP. http://www.webopedia.com/TERM/S/SOAP.html
Situation Awareness Data Link	**SADL**	An Enhanced Position Location and Reporting System (EPLRS) radio modified for use in an aircraft. SADL and EPLRS radios are used to establish a common secure tactical data link network. http://aatc.aztucs.ang.af.mil/aatcinfo.htm
Smart Card		A credit card-size device, normally for carrying and use by personnel, that contains one or more integrated circuits and also may employ one or more of the following technologies: magnetic stripe, bar codes (linear and two-dimensional), non-contact and radio frequency transmitters, biometric information, encryption and authentication, or photo identification. DoDD 8190.3, *Smart Card Technology*, 31 August 2003, Page 2, Section 3.2
Software Development Kit	**SDK**	A programming package that enables a programmer to develop applications for a specific platform; typically, an SDK includes one or more APIs, programming tools, and documentation. http://www.webopedia.com/TERM/S/SDK.html

Term	Acronym	Definition
Software Product Line	**SPL**	A software product line (SPL) is a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way. Software Engineering Institute
Spyware		Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. http://www.webopedia.com/TERM/s/spyware.html
Stakeholder		Person or organization that has a legitimate interest in a project or entity. http://en.wikipedia.org/wiki/Stakeholder
Storage		Provides physical and virtual places to host and retain data for purposes such as content staging, continuity of operations, or archival.
Sustainment		One of the two major efforts (with disposal) of the Operations and support phase of a DoD acquisition program. Sustainment includes supply, maintenance, transportation, sustaining engineering, data management, configuration management, manpower, personnel, training, habitability, survivability, environment, safety (including explosives safety), occupational health, protection of critical program information, anti-tamper provisions, and Information Technology (IT), including National Security Systems (NSS), supportability and interoperability functions. DoDI 5000.2, 12 May 2003, “Operation of the Defense Acquisition System”
System		Two or more interrelated pieces of equipment (or sets) arranged in a package to perform an operational function or to satisfy a requirement. Defense Acquisition Glossary of Terms, Jan 2001

Term	Acronym	Definition
Systems View	**SV**	A set of graphical and textual products that describes systems and interconnections providing for, or supporting, DoD functions. DoD functions include both warfighting and business functions. The SV associates systems resources to the Operational View (OV). These systems resources support the operational activities and facilitate the exchange of information among operational nodes. DoDAF v1 Vol. 1, 9 Feb 2004, pages 1-2 and 1-3, section 1.3.2
Technical Standards View	**TV**	The minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The TV includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture. DoDAF v1 Vol. 1, 9 Feb 2004, page 1-3, section 1.3.3
Transmission Control Protocol	**TCP**	One of the core protocols of the Internet Protocol (IP) suite. Using TCP, programs on networked computers can create connections to one another, over which they can send data. The protocol guarantees that data sent by one endpoint will be received in the same order by the other, without any pieces missing. It also distinguishes data for different applications (such as a Web server and an email server) on the same computer. http://en.wikipedia.org/wiki/Transmission_Control_Protocol
Transmission Control Protocol/Internet Protocol	**TCP/IP**	A suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

Term	Acronym	Definition
Transport Level Security	**TLS**	A protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet. http://www.webopedia.com/TERM/T/TLS.html
Trust Point		A trust point is a Certificate Authority (CA) that is the root of all trust for all CAs in a CA hierarchy.
Trusted Guard		Accredited to pass information between two networks at different security levels according to well defined rules and other controls. Guard products only pass defined types of information (e.g., email, images, or formatted messages). A key challenge is how to implement net-centric operations across trusted guards in the presence of CES services.
Universal Description, Discovery, and Integration	**UDDI**	An industry initiative to create a platform-independent, open framework for describing services, discovering businesses, and integrating business services using the Internet, as well as a registry. It is being developed by a vendor consortium. http://java.sun.com/j2ee/1.4/docs/glossary.html
Universal Naming Convention	**UNC**	Specifies a common syntax for accessing network resources, such as shared folders and printers. http://en.wikipedia.org/wiki/Universal_Naming_Convention
User Assistance		Provides automated “helper” capabilities and user preferences to help maximize user efficiency in task performance.
User Datagram Protocol	**UDP**	A connectionless protocol that, like TCP, runs on top of Internet Protocol (IP) networks. Unlike Transmission Control Protocol/Internet Protocol (TCP/IP), UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network. http://www.webopedia.com/TERM/U/User_Datagram_Protocol.html

Term	Acronym	Definition
Virtual Private Network	**VPN**	A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable the creation of networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. http://www.webopedia.com/TERM/V/VPN.html
Web Archive	**WAR**	A ZIP file used to distribute a set of Java classes. http://en.wikipedia.org/wiki/WAR_%28file_format%29
Web Service	**WS**	An application that exists in a distributed environment, such as the Internet. A Web Service accepts a request, performs its function based on the request, and returns a response. The request and the response can be part of the same operation, or they can occur separately, in which case the consumer does not need to wait for a response. Both the request and the response usually take the form of XML, a portable data-interchange format, and are delivered over a wire protocol, such as HTTP. http://java.sun.com/j2ee/1.4/docs/glossary.html -OR- A Web service is a software application or component that is identified by a URI and can be accessed over the Internet. It uses a vendor/platform/language-neutral data interchange format to invoke the service and supply the response. Web services use a message exchange pattern that is sufficiently well defined to be processed by a software application. Its interfaces and binding are capable of being defined, described, and discovered by XML artifacts. It supports

Term	Acronym	Definition
Web Services Atomic Transaction	**WS-AtomicTransaction**	This specification provides the definition of the atomic transaction coordination type that is to be used with the extensible coordination framework described in the WS-Coordination specification. The specification defines three specific agreement coordination protocols for the atomic transaction coordination type: completion, volatile two-phase commit, and durable two-phase commit. Developers can use any or all of these protocols when building applications that require consistent agreement on the outcome of short-lived distributed activities that have the all-or-nothing property. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/
Web Services Business Activity	**WS-BusinessActivity**	This specification provides the definition of the business activity coordination type that is to be used with the extensible coordination framework described in the WS-Coordination specification. The specification defines two specific agreement coordination protocols for the business activity coordination type: BusinessAgreementWithParticipantCompletion and BusinessAgreementWithCoordinatorCompletion. Developers can use any or all of these protocols when building applications that require consistent agreement on the outcome of long-running distributed activities. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/

Term	Acronym	Definition
Web Services Coordination	**WS-Coordination**	This specification describes an extensible framework for providing protocols that coordinate the actions of distributed applications. Such coordination protocols are used to support a number of applications, including those that need to reach consistent agreement on the outcome of distributed activities. The framework defined in this specification enables an application service to create a context needed to propagate an activity to other services and to register for coordination protocols. The framework enables existing transaction processing, workflow, and other systems for coordination to hide their proprietary protocols and to operate in a heterogeneous environment. Additionally this specification describes a definition of the structure of context and the requirements for propagating context between cooperating services. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/
Web Services Description Language	**WSDL**	An XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocols and message format to define an endpoint.
Web Services for Remote Portlets	**WSRP**	A standard for Web portals to access and display portlets that are hosted on a remote server. http://en.wikipedia.org/wiki/WSRP
Web Services Interoperability Organization	**WS-I**	An open industry organization chartered to promote Web services interoperability across platforms, operating systems and programming languages. http://www.ws-i.org/

Term	Acronym	Definition
Web Services Transaction	**WS-Transaction**	A set of specifications (WS-Coordination, WS-AtomicTransaction, and WS-BusinessActivity) that define mechanisms for transactional interoperability between Web services domains and provide a means to compose transactional qualities of service into Web services applications. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/
World Wide Web Consortium	**W3C**	Develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. W3C is a forum for information, commerce, communication, and collective understanding. http://www.w3c.org